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

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 security test, the UE initiated a 5G standalone registration by sending an Initial Registration Request to the AMF. In response, the AMF sent an Identity Request message, specifically requesting the IMEI, and crucially, this message was sent in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standards, sensitive information such as the IMEI should not be transmitted in cleartext before the security context is established, as this could expose the UE to privacy risks and device tracking. The UE, in this case, did not respond to the plain Identity Request for the IMEI, thereby refusing to transmit its IMEI in an unprotected manner. This behavior aligns with best security practices and the intent of the 3GPP standards, which aim to protect subscriber and device identities from exposure before encryption is in place. Therefore, the UE's action of withholding its IMEI until a secure context is established demonstrates a secure and standards-compliant approach to 5G NAS communication. 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 with the AMF by sending an initial registration request. In response, the AMF sent an identity request, specifically requesting the SUCI (Subscription Concealed Identifier), and this message was sent in plain (unencrypted) form. The UE then responded with an identity response, also in plain text, since the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G standard, prior to the completion of 5G-AKA, NAS messages—including the initial registration request and identity procedures—are permitted to be sent unencrypted, as security context and keys have not yet been established. The SUCI is specifically designed to protect the user's permanent identifier (SUPI) by providing a privacy-preserving, encrypted identifier that can be safely transmitted in the clear. Therefore, the UE's action of sending the SUCI in response to a plain identity request before 5G-AKA completion adheres to the 3GPP security requirements and does not expose sensitive information. Based on this, the UE's behavior in this interaction is consistent with the 5G security standard and is considered secure. Secure

3	3	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0002651214599609375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA (Authentication and Key Agreement) procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the initial NAS messages (such as registration requests and authentication challenges) are allowed to be sent in plain text before security context is established, as encryption and integrity protection can only be applied after successful authentication. The Authentication Reject message is explicitly permitted to be sent in plain text if authentication has not yet been completed. Importantly, the UE did not respond to the plain-text Authentication Reject, which is the expected and secure behavior; the UE should not proceed with further NAS procedures or attempt to establish security context after receiving an Authentication Reject. This prevents potential downgrade or replay attacks at this stage. Therefore, the UE's action—sending the initial registration request, receiving a plain-text Authentication Reject, and providing no further response—aligns with 3GPP security requirements and demonstrates secure behavior in this context. Secure
4	4	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0012979507446289062 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20431208610534668 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an initial registration request to the AMF. In response, the AMF sent an identity request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. This identity request was sent in plain (unencrypted) NAS, which is expected because the 5G-AKA authentication and key agreement procedure had not yet been completed—meaning no NAS security context was established. The UE then responded with an identity response, providing the requested SUCI. According to the 3GPP 5G standard, it is permissible for the initial NAS messages, including the identity request and response, to be sent in plain text before the security context is established, as long as the UE provides the SUCI (a privacy-preserving, encrypted version of the SUPI) rather than the cleartext SUPI. The SUCI is specifically designed to protect the subscriber's permanent identity even when sent over an unprotected channel. Therefore, the UE's action—responding with the SUCI in plain NAS before 5G-AKA completion—aligns with the security requirements of the 5G standard and does not expose sensitive information. Secure

5	5	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006351470947265625 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Protocol error, unspecified) 0.20275402069091797 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a registration reject message using 5GMM cause 111 (protocol error, unspecified) and sent this message in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. Upon receiving the registration reject, the UE responded by sending a deregistration request (UE originating) to the AMF. According to the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as there is not yet a shared key for encryption. The UE's actions—sending the initial registration request in plain text, accepting and processing the plain registration reject, and then sending a deregistration request—are consistent with expected behavior prior to the establishment of security. The UE did not attempt to send sensitive information before security activation, nor did it ignore the registration reject. Therefore, the UE's actions align with 3GPP security requirements for this stage of the NAS procedure, and there is no evidence of insecure behavior 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 test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a Registration Reject message (5GMM Cause 22: Congestion), which was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. Upon receiving the Registration Reject, the UE responded with a Deregistration Request (UE originating). According to the 3GPP 5G standard, NAS messages exchanged before the successful completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as there is no shared key material yet for encryption. The UE's action—sending a Deregistration Request in response to a Registration Reject before security context establishment—aligns with the standard, as the UE is expected to handle such rejections and can send this message in plain. Therefore, the UE's behavior in this scenario is compliant with 3GPP security requirements and does not expose any additional security risk beyond what is inherent before authentication. Secure

7	7	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 00000000000000000000000000000000 AUTN: 32303030007f0000ee555cc720560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007770061492919922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.203125 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an InitialUEMessage containing a Registration Request to the AMF. In response, the AMF sent an Authentication Request message to the UE, but this message was sent in plain (unencrypted) form and included a RAND value of all zeros and an AUTN value that appears non-standard. The UE, upon receiving this authentication request, responded with an Authentication Failure message, specifically indicating "Non-5G authentication unacceptable." According to the 3GPP 5G security standard, the authentication procedure (5G-AKA) must be properly initiated with valid parameters, and the UE is expected to reject authentication attempts that do not conform to the standard, such as those with invalid or non-random RAND values, malformed AUTN, or messages sent in plain text before security context establishment. The UE's rejection of the authentication request in this context demonstrates adherence to the 3GPP security requirements, as it did not proceed with authentication using insecure or non-compliant parameters. This behavior protects against potential security threats such as replay or downgrade attacks. Therefore, the UE's action in this scenario was secure. Secure

8	8	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 31303030000000078742b94d4550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 7 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005857944488525391 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.20240378379821777 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, controlled by the tester, responded with an Authentication Request message that was sent in plain (unencrypted) form, and notably, the 5G-AKA authentication procedure had not yet been completed. The Authentication Request included an AUTN value of all zeros, which is invalid according to 3GPP standards, and a RAND value that appears non-random or potentially malformed. Upon receiving this, the UE responded with a 5GMM status message indicating "Invalid mandatory information," rather than proceeding with authentication or responding with authentication vectors. According to 3GPP standards, the UE must not process or respond to authentication requests that are malformed, contain invalid mandatory fields, or are received before the security context is established (i.e., before 5G-AKA is completed and NAS encryption/integrity protection is activated). By refusing to process the invalid authentication request and instead reporting an error, the UE correctly avoided exposing sensitive information or proceeding with an insecure procedure. This behavior aligns with the security requirements of the 5G standard, as it prevents potential exploitation by a rogue or misconfigured AMF. Therefore, the UE's action in this scenario was secure. Secure

9	9	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03973102569580078 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003596305847168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24200010299682617 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). After completing the initial NAS steps, the UE sent an identity response to the AMF. The AMF, under test control, then sent another identity request to the UE, specifically requesting the SUCI (Subscription Concealed Identifier), and this message was sent in plain (unencrypted) form. The UE responded by providing another identity response, again in plain text, since the 5G-AKA authentication procedure had not yet been completed and therefore NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard, before the completion of 5G-AKA, identity requests and responses (including SUCI) are permitted to be sent in plain text, as the security context has not yet been established. The SUCI itself is a privacy-preserving identifier, designed to protect the subscriber's permanent identity (SUPI) even when sent in the clear. Thus, the UE's action of responding with the SUCI in plain text before the completion of 5G-AKA is compliant with the 3GPP standard and does not represent a security flaw. The UE did not expose sensitive information (such as the SUPI) in an insecure manner, and its behavior aligns with expected security procedures for this phase of the protocol. Secure

10	10	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3100 RAND: 31313131313131313131006f90d2550000 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 0.039749860763549805 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0399777889251709 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.2409358024597168 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an identity response to the AMF, the AMF replied with an authentication request message that was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. The authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI. Upon receiving this message, the UE responded with an "Authentication failure (ngKSI already in use)" message, indicating that the security context identifier (ngKSI) provided by the AMF was already in use and thus the authentication procedure could not proceed. According to the 3GPP 5G standards, the UE is required to check the validity and freshness of the ngKSI to prevent replay or reuse of security contexts, which could otherwise lead to security vulnerabilities. The UE's refusal to proceed with authentication when an already-used ngKSI is detected is a protective measure against potential attacks or misconfigurations. This behavior aligns with the security requirements of the 5G standard, as it ensures that authentication and subsequent encryption are only established under secure and unique contexts. Therefore, the UE's action in this scenario was secure. Secure
11	11	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 11 UE provided: No response The packet capture during the test using wireshark is: 0.039990901947021484 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04016995429992676 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service reject (PLMN not allowed) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). After the initial NAS steps, the UE sent an Identity Response message to the AMF, which is expected behavior when the network requests the UE's identity. At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that the security context for NAS message encryption and integrity protection was not yet established. Following the Identity Response, the AMF sent a Service Reject message with the cause "PLMN not allowed" (5GMM Cause 11), and this message was transmitted in plain (unencrypted) text. The UE did not respond further to this message. According to the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as encryption and integrity protection are only mandated after authentication is complete. The UE's behavior—sending the required Identity Response and not responding to the Service Reject—aligns with the standard and does not expose any additional security risk, since it did not transmit sensitive information after receiving the reject and before security was established. Therefore, the actions taken by the UE were in accordance with 3GPP security requirements and did not compromise security in this context. Secure

12	12	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03978896141052246 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04010796546936035 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2456059455871582 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF are engaged in the initial NAS communication phase of 5G registration, with the 5G-AKA authentication procedure not yet completed. The UE first sends an identity response to the AMF, after which the AMF issues another identity request, specifically requesting the SUCI (Subscription Concealed Identifier). The UE then responds with another identity response. Importantly, all these messages are exchanged in plain (unencrypted) form, as the 5G-AKA procedure—which establishes NAS security and encryption—has not yet occurred. According to the 3GPP 5G standard, it is expected and acceptable for identity request and response messages (such as those involving SUCI) to be sent in plain text before authentication and key agreement are completed, since the UE and network have not yet established the necessary security context. The SUCI itself is designed to protect the subscriber's permanent identity (SUPI) by encrypting it with the home network's public key, ensuring privacy even when transmitted in the clear. Therefore, the UE's actions—responding to a plain identity request with a SUCI in plain text prior to 5G-AKA—are compliant with the 3GPP security architecture and do not constitute a security breach. Secure
13	13	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.03993391990661621 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04019308090209961 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the AMF, where the UE sent an identity response message after completing the initial NAS steps. The AMF, under test control, then sent an authentication reject message to the UE in plain (unencrypted) form. According to the 3GPP 5G standard, messages exchanged before the completion of the 5G-AKA authentication procedure, such as identity requests and responses, as well as authentication reject messages, are permitted to be sent in plain text because the security context (i.e., NAS encryption and integrity protection) is not yet established. The UE, upon receiving the authentication reject message, did not respond further, which is the expected and secure behavior as specified by the standard—the UE should cease further NAS communication and not attempt to proceed with registration or authentication after receiving an authentication reject. Therefore, the UE's actions—sending the identity response in plain text before authentication and not responding to the authentication reject—are in full compliance with the 3GPP security requirements and do not expose the UE to additional risk in this context. Secure

14	14	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 22 UE provided: No response The packet capture during the test using wireshark is: 0.03981804847717285 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04005002975463867 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Registration reject (Congestion) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication where, after the initial NAS steps, the UE sent an Identity Response message to the AMF. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that the NAS security context was not established and messages were still being exchanged in plain (unencrypted) form. The AMF then responded with a Registration Reject message, also sent in plain text, with a 5GMM cause value of 22 (indicating congestion). The UE, upon receiving this Registration Reject, did not respond further. According to the 3GPP 5G standard, it is expected that before the completion of 5G-AKA, messages such as Identity Request/Response and Registration Accept/Reject are sent without NAS security protection, as the security context is not yet established. The UE's behavior—sending the Identity Response in plain text and not responding to the Registration Reject—aligns with the standard and does not expose the UE to additional security risks, since it did not proceed with any further actions that would require encryption. Therefore, the UE's actions in this scenario were secure and compliant with 3GPP specifications. Secure
15	15	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 30303030303030007844783aae550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.03972196578979492 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24048709869384766 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE responded to an identity request with an identity response, as expected. The AMF then sent an authentication request to the UE, but the message was sent in plain (unencrypted) form and contained suspicious parameters: the AUTN (authentication token) was all zeros, and the RAND (random challenge) was a non-random, predictable value. Upon receiving this, the UE immediately replied with an "Authentication failure (Non-5G authentication unacceptable)" message, indicating that it rejected the authentication attempt because it did not conform to 5G authentication requirements. According to the 3GPP 5G standard, the UE must only proceed with authentication if the parameters are valid and the procedure follows the 5G-AKA protocol, which includes proper cryptographic challenges and integrity protection. The UE's refusal to proceed with authentication in the presence of invalid or insecure parameters demonstrates adherence to the standard and protects against potential security threats such as replay or downgrade attacks. Therefore, the UE's action in this scenario was secure. Secure

16	16	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3200 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 5G-IA7 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.11983895301818848 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12023711204528809 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which is the expected behavior according to the 3GPP standards. The AMF then sent a Security Mode Command to the UE, which is the next step in establishing NAS security (ciphering and integrity protection). However, the Security Mode Command was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to 3GPP TS 24.501, the Security Mode Command must be sent as a plain NAS message because, at this point, NAS security has not yet been activated; the purpose of this message is to negotiate and activate the NAS security algorithms. The UE, upon receiving this plain Security Mode Command, did not respond. This lack of response could indicate that the UE is programmed to reject or ignore plain NAS messages at this stage, possibly as a security measure to avoid accepting potentially spoofed or replayed commands. However, according to the 3GPP standard, the UE is expected to process the plain Security Mode Command and respond with a Security Mode Complete message, also sent in plain NAS, to complete the security activation. By not responding, the UE deviates from the standard procedure, but this action could be interpreted as a conservative security posture, possibly to prevent attacks exploiting weaknesses in the plain message phase. However, strictly from a standards compliance perspective, the UE's lack of response is not in line with 3GPP specifications, which require the UE to process and respond to the plain Security Mode Command. Therefore, while the UE's action may be cautious, it is considered "insecure" in terms of standards compliance, as it prevents the proper establishment of NAS security and could lead to denial of service. 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 5G standalone User Equipment (UE) initiated NAS communication and, after completing the initial steps, 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 mutual authentication and the establishment of NAS security (encryption and integrity protection) had not occurred. The AMF, under test control, responded with a Service Reject message, sent in plain (unencrypted) text, with a 5GMM cause of 111 (Protocol error, unspecified). According to 3GPP 5G standards, prior to the completion of 5G-AKA, all NAS messages are expected to be sent in plain text, as security contexts have not yet been established. The UE, upon receiving the Service Reject message, did not respond further, which is appropriate since the service was explicitly rejected and the message was sent in plain text as per protocol before security activation. Therefore, the UE's actions—sending the Authentication Response in plain text before security activation and not responding to a Service Reject—are consistent with 3GPP security requirements and do not expose the UE to additional risk in this context. The UE did not act insecurely in this exchange. Secure

18	18	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 4.243709087371826 UE to AMF SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, Authentication response 4.243997097015381 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Identity request 4.445895195007324 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE completed the initial NAS steps and sent an authentication response to the AMF, the AMF (under test control) sent an identity request for the SUCI (Subscription Concealed Identifier) to the UE. Importantly, this identity request was sent in plain (unencrypted) NAS, as the 5G-AKA procedure had not yet been completed, meaning NAS security context was not established. The UE responded with an identity response, also in plain NAS. According to the 3GPP 5G security standard (TS 33.501), before the completion of 5G-AKA, NAS messages are permitted to be sent in plain text, as security context and ciphering have not yet been established. The SUCI itself is designed to protect the permanent subscriber identity (SUPI) even when sent over an unprotected channel, as it is a privacy-preserving, encrypted identifier. Therefore, the UE's action—responding with the SUCI in plain NAS prior to security context establishment—aligns with the 3GPP standard and does not expose sensitive information. Based on this, the UE's behavior in this scenario is considered secure. Secure
19	19	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11986708641052246 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12012410163879395 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3239710330963135 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successfully completing the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was integrity protected and indicated the use of the 5G-EA0 (null) ciphering algorithm and 128-5G-IA2 for integrity protection. The security header specified that the message was integrity protected with a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standards, after authentication, the UE and network must agree on security algorithms for both ciphering and integrity protection. The use of 5G-EA0 (null ciphering) means that no encryption would be applied to subsequent NAS messages, which is generally only allowed in exceptional cases (such as emergency calls or when no other algorithm is supported). If the UE supports stronger ciphering algorithms but is instructed to use 5G-EA0 in a normal context, it is expected to reject the security mode command to prevent unencrypted communication, thereby protecting user data and signaling from potential interception. The UE's decision to reject the security mode command when only null ciphering was proposed aligns with secure behavior as defined by 3GPP, ensuring that communication does not proceed without proper encryption. Therefore, the UE's action 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 completed the initial NAS procedures and sent an authentication response to the AMF. However, instead of progressing to the next stage of the 5G-AKA authentication and key agreement procedure, the AMF sent another authentication request to the UE, and this message was sent in plain (unencrypted) form. The UE, upon receiving this second authentication request, responded with another authentication response. According to the 3GPP 5G security standard, NAS messages containing authentication information (such as authentication response) should only be sent in plain text before the security context is established, i.e., before the 5G-AKA procedure is completed. After the successful completion of 5G-AKA, all subsequent NAS messages must be integrity protected and, where required, encrypted. In this test, since the 5G-AKA procedure was not completed, the UE was correct in sending its authentication response in plain text. However, the unusual aspect is that the AMF sent a second authentication request after already receiving a response, which is not standard behavior and could indicate a replay or protocol anomaly. The UE, by responding again in plain text before security context establishment, is still acting within the expected 3GPP protocol, as it cannot enforce encryption until keys are derived. Therefore, based on the 3GPP standard, the UE's actions were secure, as it did not prematurely encrypt or integrity-protect messages before the security context was established, and it followed the expected protocol flow for the state it was in. Secure

21	21	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 303030303030300078d431f251560000 AUTN: 4953cc15a85a90008f0a1f4e8f0a3310 ngKSI_TSC: Native security context ngKSI_KSI: 4 UE provided: Authentication failure (MAC failure) The packet capture during the test using wireshark is: 1.8795151710510254 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, Authentication response 1.8797390460968018 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication request 2.0836050510406494 UE to AMF UplinkNASTransport, Authentication failure (MAC failure) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication as part of the 5G-AKA authentication procedure. After the UE sent an authentication response, the AMF, under test control, sent another authentication request in plain (unencrypted) form, even though the 5G-AKA procedure had not yet been completed and security context was not established. The UE, upon receiving this authentication request, responded with an "Authentication failure (MAC failure)" message, indicating that it detected an integrity failure in the received message, specifically a mismatch in the Message Authentication Code (MAC). According to the 3GPP 5G security standards, the UE is required to verify the integrity of authentication messages using the MAC and to reject any message with an invalid MAC to prevent replay or tampering attacks. By refusing to proceed and signaling a MAC failure, the UE correctly followed the 3GPP security procedures, ensuring that it did not accept potentially malicious or tampered authentication requests. This behavior demonstrates that the UE was operating securely 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: 313131313131313310057a1d8550000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.11977601051330566 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999082565307617 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.3230268955230713 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, which then replied with another authentication request message sent in plain (unencrypted) form. The UE subsequently responded with an "Authentication failure" message, specifically indicating "Non-5G authentication unacceptable." According to the 3GPP 5G security standards, the 5G-AKA (Authentication and Key Agreement) procedure must be successfully completed before any NAS messages can be securely encrypted and integrity protected. If the AMF sends a subsequent authentication request in plain text after the authentication response, this is not compliant with the expected 5G security procedures. The UE, recognizing that the authentication process was not proceeding according to 5G standards (possibly due to the message being unprotected or the authentication vectors being reused or invalid), correctly rejected the authentication attempt by sending an authentication failure message. This behavior aligns with the 3GPP specifications, which require the UE to reject non-standard or insecure authentication procedures to prevent downgrade or replay attacks. Thus, the UE's action in refusing to proceed with a non-5G-compliant authentication process demonstrates adherence to security best practices as outlined by the standard. Secure

23	23	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11994004249572754 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12018203735351562 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.32151198387145996 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an authentication response to the AMF, which then issued a Security Mode Command to the UE. The Security Mode Command specified the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm, with the security header indicating integrity protection with a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G security standards (TS 33.501), after authentication, the UE and the network must negotiate mutually acceptable ciphering and integrity algorithms to protect NAS messages. The use of the null ciphering algorithm (5G-EA0) means that messages would not be encrypted, only integrity protected. The 5G standard allows the UE to reject the Security Mode Command if it does not accept the proposed security algorithms, especially if the network proposes to use no encryption (EA0) when the UE expects confidentiality. The UE's rejection of the Security Mode Command under these circumstances is a secure and standards-compliant action, as it prevents the establishment of a security context that would leave NAS messages unencrypted and potentially vulnerable to interception. Therefore, the UE acted securely by refusing to proceed with a null ciphering algorithm. Secure

24	24	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 5781adc4c6cd42baaf6e4fe6cef2e17f AUTN: 67373384aeb990006bc203d2c023b868 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication response The packet capture during the test using wireshark is: 0.11973094940185547 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12026000022888184 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.32166409492492676 UE to AMF UplinkNASTransport, Authentication response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, which then replied with a new authentication request sent in plain (unencrypted) form. The UE subsequently responded again with another authentication response, even though the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed. According to the 3GPP 5G security standard, the UE should only respond to authentication requests that are part of the expected authentication sequence and should be cautious when receiving unexpected or repeated authentication requests, especially if they are sent in plain text after an authentication response has already been provided. The fact that the UE responded to a repeated authentication request sent in plain text, before the security context was established, exposes it to potential replay or man-in-the-middle attacks. The UE should have rejected or ignored the repeated authentication request, as responding to such messages before the completion of 5G-AKA and the establishment of a secure context is not compliant with 3GPP security best practices. Therefore, the action taken by the UE in this scenario is considered insecure. Insecure
25	25	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 1.3825318813323975 UE to AMF UplinkNASTransport, Authentication response 1.3827719688415527 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication reject 1.3827838897705078 UE to AMF SACK (Ack=2, Arwnd=106469) , UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and the AMF were engaged in the NAS authentication procedure as part of the 5G-AKA process. After the UE sent its authentication response, the AMF replied with an authentication reject message, which was sent in plain (unencrypted) form because the 5G-AKA procedure had not yet been completed and security context was not established. Upon receiving the authentication reject, the UE did not attempt to proceed with further registration or protected communication; instead, it immediately sent a deregistration request to the AMF, effectively terminating its attempt to connect to the network. According to the 3GPP 5G standards, if authentication fails or is rejected before security context establishment, the UE should not proceed with any further sensitive operations and should cease registration attempts. The UE's behavior—terminating the session after receiving an authentication reject and not sending any further NAS messages that would require encryption—aligns with these security requirements. This prevents exposure of sensitive information over an unprotected channel and mitigates potential security risks. Therefore, the UE's actions in this scenario were secure and compliant with the 5G standard. Secure

26	26	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.15973997116088867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15994787216186523 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.3668229579925537 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the User Equipment (UE) sent a Security Mode Complete message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to use them for subsequent NAS communication. Following this, the AMF sent a Deregistration Request message to the UE, which was integrity protected and ciphered, as indicated by the security header (value 2). The UE then responded with a Deregistration Accept message, also protected by the established security context. According to the 3GPP 5G standards, specifically TS 24.501, after the security context is established via 5G-AKA and Security Mode Command/Complete exchange, all subsequent NAS messages—including deregistration procedures—must be both integrity protected and ciphered. The packet capture confirms that the UE only sent protected messages after security activation, and it responded appropriately to the AMF's deregistration request. There is no indication that the UE accepted or responded to any unprotected or suspicious messages, nor did it proceed with deregistration before security was established. Therefore, the UE's actions were in line with 3GPP security requirements, maintaining the confidentiality and integrity of NAS signaling as expected. Secure
27	27	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.1597728729248047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16001200675964355 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.36782288551330566 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) first completed the 5G-AKA authentication procedure, which is a prerequisite for establishing a secure NAS (Non-Access Stratum) communication channel. Following this, the UE sent a "security mode complete" message, indicating that it had accepted the security parameters negotiated with the Access and Mobility Management Function (AMF). Immediately after, the AMF sent a "deregistration request" message to the UE, which was protected with both integrity and ciphering, as indicated by the security header (value 2). The UE responded with a "deregistration accept" message, acknowledging the deregistration request. According to the 3GPP 5G standards, once 5G-AKA is completed and security mode is established, all subsequent NAS messages, including deregistration procedures, must be protected using the agreed security context (integrity protected and ciphered). 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 ciphered deregistration request after security context establishment, its actions align with the 3GPP security requirements and do not expose it to known security vulnerabilities such as accepting unprotected deregistration requests. Therefore, the UE's behavior in this scenario is compliant with the 5G security standards. Secure

28	28	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.16000795364379883 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602778434753418 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36232805252075195 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the proposed security algorithms and was ready to establish a secure NAS communication context. However, the AMF then sent another "security mode command" message, this time protected, specifying the use of ciphering algorithm 128-5G-EA2 and integrity algorithm 5G-IA0 (null integrity protection). The UE responded by rejecting this security mode command with a "security mode reject" message, citing an unspecified reason. According to the 3GPP 5G standard, the use of a null integrity algorithm (5G-IA0) is generally discouraged for NAS signaling, as it leaves messages vulnerable to tampering and replay attacks. The UE's action to reject a security context that does not provide integrity protection aligns with best security practices and the intent of the standard, which is to ensure both confidentiality and integrity of NAS messages. By refusing to accept a security mode that would have left its communication without integrity protection, the UE demonstrated secure behavior in accordance with the 5G security requirements. Secure

29	29	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.15992307662963867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16016101837158203 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36194396018981934 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA (authentication and key agreement), the UE sent a "security mode complete" message to the AMF, indicating its readiness to proceed with protected NAS communication. However, the AMF then sent a "security mode command" back to the UE, specifying the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, but with a security header indicating "integrity protected with new security context." Upon receiving this, the UE responded with a "security mode reject" message, citing an unspecified reason for rejection. According to the 3GPP 5G standards, after successful authentication, the UE and network are expected to negotiate and use strong ciphering and integrity protection algorithms to secure NAS signaling. The use of null algorithms (EA0/IA0) after authentication is considered insecure and is only permitted in very limited, specific scenarios (e.g., emergency services or certain test cases). The UE's rejection of the security mode command that attempted to establish a null security context after authentication demonstrates that it is adhering to the security requirements of the standard by refusing to operate in an insecure mode. Therefore, the UE's action was secure, as it protected itself from being downgraded to an insecure communication mode. Secure

30	30	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected (1) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.16007494926452637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037607192993164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.364534854888916 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms (5G-EA7 for ciphering and 128-5G-IA2 for integrity protection) and was ready to begin protected NAS communication. However, the AMF, under test control, responded with another "security mode command" message, which is an unexpected behavior according to the 3GPP 5G standard (TS 24.501). The UE, upon receiving this second security mode command, again sent a "security mode complete" message. According to the 3GPP standard, once the security context is established and the UE has acknowledged it with "security mode complete," all subsequent NAS messages must be integrity protected and, if required, ciphered. The UE's action of accepting and responding to a second security mode command after already completing the security mode procedure is not compliant with the standard; the UE should have rejected or ignored the redundant security mode command, as it could indicate a protocol error or a potential security attack (such as a replay or downgrade attempt). By responding to the second security mode command, the UE potentially exposes itself to security risks, as this behavior could be exploited by an attacker to disrupt the security context or attempt to downgrade the security algorithms. Therefore, the UE's action in this scenario was not secure according to the 3GPP 5G standard. Insecure

31	31	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3300 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.1600170135498047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16026687622070312 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36418795585632324 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security algorithms and the establishment of a new security context. Immediately following this, the AMF sent a "security mode command" message to the UE, which was protected (i.e., integrity protected and/or ciphered) as per the negotiated security parameters: ciphering with 5G-EA4 and integrity protection with 5G-IA0 (null integrity). The UE then sent a deregistration request (UE originating) to the AMF. According to the 3GPP 5G security standard, after the security mode command is completed and the security context is established, all subsequent NAS messages from the UE should be protected using the agreed ciphering and integrity algorithms. In this case, the integrity algorithm used was 5G-IA0, which is a null algorithm, meaning that while the messages are encrypted, they are not integrity protected. This is generally not recommended for commercial deployments, as it leaves the messages vulnerable to modification attacks, but it is permitted by the standard for certain scenarios (e.g., for testing or in specific regulatory environments). The UE correctly followed the security procedures by waiting for the security context to be established before sending sensitive messages (like deregistration request), and it used the negotiated algorithms as instructed by the AMF. However, the use of 5G-IA0 (null integrity) means the communication lacks integrity protection, which is a security risk according to best practices, even if technically allowed by the standard. Therefore, while the UE's actions were compliant with the protocol and the test configuration, the lack of integrity protection makes the communication insecure from a practical security perspective. 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, the 5G-AKA authentication procedure was completed, establishing the necessary security context for protected NAS communication between the User Equipment (UE) and the Access and Mobility Management Function (AMF). After completing the initial NAS steps, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security algorithms and parameters negotiated during the security mode command. However, the AMF then sent another "security mode command" message to the UE, this time as a protected (integrity protected and ciphered) message, using the agreed cipher (5G-EA4) and integrity (128-5G-IA3) algorithms. According to the 3GPP 5G standard, once the security context is established and the security mode complete message is sent, the UE should not expect to receive a new security mode command unless there is a justified context re-establishment or handover scenario. Receiving a second security mode command after security activation is considered abnormal and could indicate a replay or downgrade attack attempt. The UE, in this case, did not respond to the unexpected protected security mode command, which aligns with 3GPP security recommendations to ignore or silently discard such abnormal or potentially malicious messages to prevent security vulnerabilities. By refusing to process or respond to the second security mode command, the UE demonstrated 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 request 0.1606900691986084 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Illegal ME) 0.36391305923461914 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to use protected NAS signaling. 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 status, the UE responded by sending a Deregistration Request (UE originating), indicating that it was initiating deregistration from the network. According to the 3GPP 5G standard (TS 24.501), after security activation, all subsequent NAS messages—including status and deregistration—should be integrity protected and, if required, ciphered. The packet capture indicates that the messages exchanged after 5G-AKA completion were protected, as expected. The UE's action to deregister upon receiving an "Illegal ME" cause is also compliant with the standard, as the UE should not attempt to continue registration if the network indicates that the device is not allowed. Therefore, the UE's behavior in this scenario was both secure and compliant with the 3GPP 5G standard, as it maintained protected communication and responded appropriately to the network's status message. 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) (Undocumented) 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, the 5G standalone User Equipment (UE) first completed the 5G-AKA authentication procedure, establishing a secure context for NAS message protection. Following this, the UE sent a "security mode complete" message, indicating that it had successfully negotiated and activated NAS security (integrity and ciphering) with the Access and Mobility Management Function (AMF). Subsequently, the AMF sent a "deregistration request" message to the UE, which was observed to be protected with both integrity and ciphering, as indicated by the security header (2). The UE then responded with a "deregistration accept" message, also under the established security context. According to the 3GPP 5G standard, after the completion of 5G-AKA and security mode command/complete exchange, all subsequent NAS messages between the UE and AMF must be integrity protected and ciphered to prevent eavesdropping and tampering. The packet capture confirms that the UE only sent sensitive messages (such as deregistration accept) after security was activated, and all messages were properly protected. Therefore, the UE's actions adhered to the security requirements outlined by 3GPP, ensuring that no sensitive information was transmitted in the clear and that the communication was robust against common security threats. Secure
35	35	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.15990018844604492 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16015410423278809 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it 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 observed to be protected (i.e., integrity protected and/or ciphered as per 3GPP standards). However, the UE did not respond to the protected "service accept" message from the AMF. According to the 3GPP 5G NAS protocol (TS 24.501), after the security mode is completed and NAS security is activated, all subsequent NAS messages between the UE and the AMF must be protected. The UE is expected to process protected messages from the AMF and respond appropriately. The lack of response from the UE to a properly protected "service accept" message suggests that the UE either failed to process the message or did not recognize it as valid, which is not compliant with the expected behavior as per the 5G standard. This could indicate a security or implementation flaw in the UE, as it should be able to handle protected messages after security activation. Therefore, based on the 3GPP standard and the observed behavior, the UE's action in this scenario is considered insecure. Insecure

36	36	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5051651000976562 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5054340362548828 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7091829776763916 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, 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 was established and subsequent NAS messages would be protected. The AMF, under test control, then sent a "Deregistration Request (UE terminated)" message to the UE, which was observed to be integrity protected and ciphered, as indicated by the security header. The UE responded appropriately with a "Deregistration Accept (UE terminated)" message, completing the deregistration process. According to the 3GPP 5G standard, after the 5G-AKA procedure, all NAS signaling messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered to ensure confidentiality and authenticity. The UE's actions—responding only after security was established and sending the correct deregistration response—demonstrate compliance with these security requirements. The UE did not process or respond to any unprotected or insecure messages, and all communications after authentication were properly protected. Therefore, based on the observed behavior and adherence to 3GPP security procedures, the UE's actions in this interaction were secure. Secure
37	37	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5078079700469971 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5080060958862305 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Service accept 0.7117960453033447 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that it had finished the registration process. The AMF then responded with a "Service Accept" message, which was sent as a protected (i.e., integrity protected and/or ciphered) NAS message, confirming that security context was established and NAS security was active. Following this, the UE sent a "Deregistration Request (UE originating)" message to the AMF. According to the 3GPP 5G standards, once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected using the negotiated security context. The packet capture shows that the "Service Accept" message from the AMF was protected, which implies that the security context was in use. Since the UE sent the "Deregistration Request" only after the security context was established and NAS security was active, and there is no indication that the UE sent any unprotected NAS messages after authentication, the UE's actions are in line with 3GPP security requirements. Therefore, the UE's communication in this scenario can be considered secure. Secure

38	38	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.5716309547424316 UE to AMF UplinkNASTransport, Registration complete 0.5718338489532471 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS procedures were finished. Subsequently, the AMF sent a "Security Mode Command" message to the UE, which was protected with integrity using the newly established security context (as indicated by the security header type 3) and specified the use of the null cipher algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm. The UE, upon receiving this command, did not respond. According to the 3GPP 5G standard, after 5G-AKA, the AMF initiates the Security Mode Command to establish NAS security, and the UE is expected to respond with a Security Mode Complete message if it accepts the proposed algorithms and context. The use of the null cipher (EA0) is permitted by the standard, but the UE must be able to handle this scenario securely, including verifying the integrity protection and responding appropriately. The fact that the UE did not respond to a properly protected Security Mode Command, even with null ciphering, suggests that it failed to comply with the expected behavior outlined by 3GPP, potentially leaving the connection in an insecure or undefined state. This lack of response could indicate a security weakness or implementation flaw, as the UE should at least respond with a Security Mode Reject if it cannot accept the parameters. Therefore, the UE's action in this scenario was not secure according to the 5G standard. Insecure
39	39	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.2683730125427246 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2686209678649902 AMF to UE SACK (Ack=12, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.476357936859131 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "registration complete" message to the AMF, indicating that the initial NAS security context was established. Following this, the AMF sent a "configuration update command" to the UE, which was protected with both integrity and ciphering, as indicated by the security header (value 2). The UE then responded with a "configuration update complete" message. According to the 3GPP 5G standards (TS 24.501), after successful authentication and security mode command, all subsequent NAS messages exchanged between the UE and AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The packet capture confirms that the downlink configuration update command from the AMF was indeed protected, and the UE responded appropriately within the secured context. Since the UE only sent messages after the security context was established and responded to protected messages as required by the standard, the actions taken by the UE were in line with 3GPP security requirements. Therefore, based on the information provided and the sequence of events, the UE's communication was secure. Secure

40	40	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.427475929260254 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.427738904953003 AMF to UE SACK (Ack=12, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.6314868927001953 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "registration complete" message to the AMF, indicating that it had finished the registration process. Subsequently, the AMF sent a "configuration update command" to the UE, which was observed in the packet capture as being protected with both integrity protection and ciphering, as indicated by the security header (2). The UE then responded with a "configuration update complete" message, confirming receipt and processing of the command. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be both integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The packet capture and message flow confirm that the UE only responded to a protected (integrity protected and ciphered) configuration update command and did not process any unprotected or insecure messages after security activation. This behavior aligns with the security requirements of the 5G standard, as the UE did not accept or respond to any unprotected NAS signaling after the establishment of a security context. Therefore, the actions taken by the UE in this interaction were secure and compliant with 3GPP specifications. Secure

41	41	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0272 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 6.938914060592651 UE to AMF UplinkNASTransport, Registration complete 6.939129114151001 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Security mode command 7.142905950546265 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 7.143115997314453 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security procedures had been completed. The AMF then sent a "Security Mode Command" message, which was properly protected (integrity protected with a new security context, using 128-5G-EA2 for ciphering and 128-5G-IA2 for integrity). However, the UE did not respond to this security mode command. Subsequently, the UE attempted to send a "Service Request" (InitialUEMessage) to the AMF, which was rejected by the network because the UE identity could not be derived. According to the 3GPP 5G standard, after receiving a Security Mode Command, the UE is required to process the command, activate the indicated security algorithms, and respond with a Security Mode Complete message before sending any further NAS messages. The absence of a response from the UE to the Security Mode Command, followed by the transmission of a Service Request, is a deviation from the standard and represents insecure behavior. This is because the UE should not send further NAS messages until the security context is established and confirmed, as this could expose the communication to security vulnerabilities. Therefore, the UE's actions in this scenario were not in compliance with 3GPP security procedures. Insecure
42	42	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.513239860534668 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5140058994293213 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5144908428192139 AMF to UE DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending a Deregistration Accept message back to the UE. The Deregistration Accept message from the AMF was sent as a protected (i.e., integrity protected and/or ciphered) NAS message, as required after 5G-AKA completion. The UE, upon receiving this protected Deregistration Accept message, did not respond further. According to the 3GPP 5G standard (TS 24.501), after the UE receives a Deregistration Accept message (especially when the deregistration was initiated by the network or the UE), it is not required to send any further NAS messages and should proceed to release its NAS signaling connection and perform local deregistration procedures. The fact that the UE did not respond to the protected Deregistration Accept message is therefore in line with the expected and secure behavior as specified by the standard. The UE only sent NAS messages after the 5G-AKA was completed, ensuring that all subsequent NAS communications were protected, which is compliant with 3GPP security requirements. Thus, the UE's actions in this scenario were secure. Secure

43	43	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5069518089294434 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5071558952331543 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5073068141937256 AMF to UE DownlinkNASTransport 0.7109389305114746 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test scenario, the 5G-AKA authentication procedure was completed first, establishing a secure context between the User Equipment (UE) and the Access and Mobility Management Function (AMF). Following this, the UE sent an Uplink NAS Transport message, after which the AMF responded with a Configuration Update Command. The packet capture shows that the Configuration Update Command from the AMF was sent as a protected message, specifically with a security header indicating that it was both integrity protected and ciphered, which means it was encrypted and authenticated as per 3GPP 5G security standards. After receiving this protected message, the UE responded with a Deregistration Request (UE originating), which is a legitimate action if the UE wishes to deregister or if it detects an unexpected or suspicious configuration update. According to 3GPP standards, once 5G-AKA is completed, all subsequent NAS messages must be integrity protected and ciphered to ensure confidentiality and authenticity. The UE's actions—receiving and processing only protected messages and responding appropriately—demonstrate adherence to these security requirements. There is no evidence in the trace of the UE accepting or acting upon unprotected or unauthenticated messages, nor is there any indication of the UE sending sensitive information in the clear. Therefore, based on the observed behavior and adherence to the 3GPP security requirements, the UE's actions in this scenario were secure. Secure
44	44	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 6.589772939682007 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.5903379917144775 AMF to UE SACK (Ack=18, Arwnd=106401) , DownlinkNASTransport, Configuration update command 6.590748071670532 AMF to UE DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 6.793751955032349 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE proceeded with normal NAS communication, sending uplink NAS transport messages to the AMF. Following these exchanges, the AMF (under test control) sent a deregistration request to the UE, which was integrity protected and ciphered, as indicated by the security header (2). The UE responded appropriately with a deregistration accept message, indicating that it processed the request as a legitimate, protected command and terminated its registration as instructed. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages must be integrity protected and ciphered to ensure confidentiality and authenticity. The UE only responded to a properly protected deregistration request, which aligns with the expected secure behavior defined by the standard. The UE did not act on any unprotected or suspicious messages and only accepted a deregistration request that was cryptographically secured, demonstrating adherence to the security requirements. Therefore, based on the observed actions and the 3GPP security guidelines, the UE's behavior in this scenario was 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 completing the 5G-AKA authentication and key agreement procedure, the UE sent an Uplink NAS Transport message to the AMF, indicating that the security context was established and NAS security should be active. The AMF then sent a Configuration Update Command to the UE, which, according to the packet capture, was protected with both integrity protection and ciphering (security header type 2), as required by 3GPP TS 33.501 for NAS messages following successful authentication. The UE responded with a Configuration Update Complete message, also sent as a NAS message after security activation. Since all subsequent NAS messages after 5G-AKA completion were integrity protected and ciphered, and the UE properly responded to the protected Configuration Update Command, the UE's actions align with 3GPP security requirements. The UE did not send or accept any unprotected NAS messages after security activation, and there is no evidence of security context misuse or protocol deviation. Therefore, based on the interaction and adherence to 3GPP standards, the UE's actions were secure. Secure
46	46	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.425251007080078 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4254679679870605 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4255969524383545 AMF to UE DownlinkNASTransport, Configuration update command 2.629240036010742 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated an Uplink NAS Transport message, which was followed by the AMF sending a Configuration Update Command. According to the packet capture, the Configuration Update Command sent by the AMF was protected using both integrity protection and ciphering, as indicated by the security header (2), which aligns with 3GPP requirements that mandate NAS messages be protected after security context establishment. The UE then responded with a Configuration Update Complete message, which was also sent after security activation. Since the 5G-AKA procedure was completed before these exchanges, both uplink and downlink NAS messages were expected to be encrypted and integrity protected. The UE's actions—accepting and responding to a protected Configuration Update Command only after security was established—are in line with the 3GPP 5G security standards (TS 33.501), which require that sensitive NAS procedures occur only after security activation. Therefore, the UE's behavior in this interaction demonstrates adherence to the expected security protocols for 5G standalone operation. Secure

47	47	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.4281399250030518 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4283440113067627 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.428462028503418 AMF to UE DownlinkNASTransport, Configuration update command 2.6321370601654053 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the security context is now established. The AMF then sent a Configuration Update Command to the UE, which, according to the packet capture, was transmitted as a protected message with both integrity protection and ciphering enabled (security header type 2). The UE responded with a Configuration Update Complete message, indicating that it processed the command as required. According to the 3GPP 5G security standards (TS 33.501), after the 5G-AKA procedure, all subsequent NAS messages between the UE and the AMF must be both integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The packet capture confirms that the downlink Configuration Update Command from the AMF was indeed protected, and the UE responded appropriately. Since the UE only sent and responded to messages after the security context was established and did so using protected NAS signaling, the UE's actions align with the 5G security requirements. Therefore, the UE's behavior in this interaction was secure. Secure

48	48	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3200 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 2.4352028369903564 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4353890419006348 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.435595989227295 AMF to UE DownlinkNASTransport, Security mode command 2.6392359733581543 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, indicating that the initial security context should have been established. The AMF then sent a Security Mode Command to the UE, which was protected (integrity protected with a new security context) and specified the use of ciphering and integrity algorithms (5G-EA4 and 128-5G-IA2), as well as the ABBA parameter. Upon receiving this command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, after 5G-AKA, the UE is expected to accept the Security Mode Command if the parameters are supported and the message is valid and properly protected. A Security Mode Reject is only expected if the UE detects an issue such as an unsupported algorithm, an invalid or established message, or a mismatch in security context. Since the Security Mode Command was sent as protected and the algorithms specified are standard, the UE's rejection without a specific reason (unspecified) suggests either a failure to process the message correctly or a potential misconfiguration in the UE's security handling. If the UE rejected the Security Mode Command due to a legitimate security concern (e.g., unsupported algorithm or integrity failure), this would be secure behavior. However, since the rejection was unspecified and the message was properly protected, this action may indicate a lack of compliance with the 3GPP standard or a failure to interoperate securely. Therefore, based on the information provided and the expectation that the UE should accept a valid, protected Security Mode Command after 5G-AKA, the UE's action appears to be insecure. 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 successfully completing the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF 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, with the security header set to "Integrity protected with new security context." Upon receiving this command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard (TS 33.501), after 5G-AKA, the network and UE should negotiate security algorithms for both integrity and ciphering protection. The use of 5G-EA0 (null ciphering) means that user data would not be encrypted, which is generally only allowed in specific, controlled scenarios (such as emergency services or regulatory requirements). For normal operation, the UE is expected to reject a Security Mode Command that mandates null ciphering, as this would expose user data to potential interception. The UE's action to reject the security mode command under these circumstances aligns with the security requirements of the 5G standard, as it prevents the establishment of an insecure connection. Therefore, the UE's behavior in this test was secure. Secure
50	50	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 24.788990020751953 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 24.789222955703735 AMF to UE SACK (Ack=27, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a service request to the AMF, which is a standard procedure for requesting network services. In response, the AMF sent a "deregistration accept" message to the UE, and this message was protected (i.e., integrity protected and/or encrypted), as expected after 5G-AKA completion. Notably, the UE did not respond to the protected deregistration accept message from the AMF. According to the 3GPP 5G standards, after the security context is established (post-5G-AKA), all NAS signaling messages must be integrity protected and, where applicable, encrypted. The UE is required to process protected messages and respond appropriately. The lack of response from the UE to a valid, protected deregistration accept message indicates that the UE did not follow the expected protocol behavior, which could lead to security or service issues (e.g., the UE may remain registered when it should not, or may be vulnerable to replay or denial-of-service attacks if it does not handle deregistration properly). Therefore, the UE's action in this scenario—failing to respond to a protected, standards-compliant message—does not align with the secure behavior outlined by 3GPP specifications. Insecure

51	51	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 25.642455101013184 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 25.642899990081787 AMF to UE SACK (Ack=24, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Message type not compatible with the protected 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 security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, indicating a desire to initiate a service (such as mobile-originated data). In response, the AMF sent a Deregistration Request (UE terminated) message, which was integrity protected and ciphered, meaning it was both encrypted and authenticated as per 3GPP security requirements. The UE, upon receiving this protected message, responded with a Deregistration Accept (UE terminated), acknowledging the deregistration as requested. According to 3GPP standards, after the security context is established (post-5G-AKA), the UE must only accept and respond to NAS messages (Message type not compatible with the protected state) ciphered) and must follow protocol state machines. In this scenario, although the Deregistration Request was sent in a state where it may not be expected (immediately after a Service Request), the UE correctly processed the protected message and responded appropriately, as required by the standard. The UE did not accept or respond to any unprotected or suspicious messages, and only acted on a message that was securely delivered after authentication. Therefore, the UE's actions were secure and compliant with 3GPP 5G security specifications. 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 5G-AKA authentication, the UE initiated a service request, which is a standard procedure to request access to network services. The AMF, under tester control, responded with a configuration update command, which was sent as a protected NAS message (integrity protected and ciphered, as indicated by security header type 2). Upon receiving this, the UE responded with a deregistration request (UE originating), also sent as an uplink NAS message. Since the 5G-AKA procedure was completed before these exchanges, both the service request and the subsequent messages were protected by NAS security, ensuring confidentiality and integrity as per 3GPP standards. The UE's action to send a deregistration request in response to a protected configuration update command does not, by itself, indicate a security flaw; it may reflect a policy or implementation decision, such as rejecting an unexpected or unsupported configuration update. Importantly, all sensitive NAS messages after authentication were properly protected, and there is no evidence of the UE sending unprotected or insecure messages post-authentication. Therefore, based on the 3GPP 5G security requirements and the observed message flow, the UE's actions were secure. Secure

53	53	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 17.000593185424805 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.001089096069336 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal UE) 17.204612970352173 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication and security setup, the UE initiated a service request, which is a standard procedure for requesting network services. The AMF, under the tester's control, responded with a deregistration request (UE terminated), which was integrity protected and ciphered, indicating that NAS security was active and the message was encrypted and authenticated as per 3GPP 5G standards. The UE, upon receiving this protected deregistration request, responded with a deregistration accept message, completing the deregistration procedure. According to 3GPP TS 24.501, once NAS security is established, the UE is required to process and respond to protected NAS messages, including deregistration requests, even if the deregistration is unexpected or initiated by the network. The UE's actions—processing a properly protected deregistration request and responding accordingly—demonstrate compliance with the 5G security procedures. There is no indication that the UE accepted any unprotected or invalid messages, nor did it behave in a way that would compromise security. Therefore, based on the information provided and the 3GPP requirements, the UE's actions in this scenario were secure. Secure
54	54	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 100 UE provided: No response The packet capture during the test using wireshark is: 1.321023941040039 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.3216829299926758 AMF to UE DownlinkNASTransport, 5GMM status (Conditional IE error) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a Service Request, which was transmitted to the AMF. The AMF, in response, sent a protected (i.e., integrity protected and/or ciphered) GMM Status message with a 5GMM Cause value of 100, indicating a "Conditional IE error." According to the 3GPP 5G standard, specifically TS 24.501, when the UE receives a GMM Status message with a cause value it does not recognize or that indicates an error, the UE is not required to respond, particularly if the message is protected and the cause does not require a corrective action from the UE. The UE's decision to provide no response is in line with the 3GPP specification, which states that the UE may ignore certain status messages, especially if they are protected and do not necessitate further action. This behavior helps prevent unnecessary signaling and potential security vulnerabilities that could arise from responding to unexpected or malformed messages. Therefore, the UE's action in this scenario was secure and compliant with 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 test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form before the 5G-AKA authentication procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the initial NAS messages, including the registration request and the authentication reject, are allowed to be sent without encryption or integrity protection because the mutual authentication and key establishment (5G-AKA) have not yet occurred. The UE, upon receiving an Authentication Reject message in plain text before security context establishment, is expected to not respond further, as per the standard, to prevent any further exposure or risk. In this test, the UE did not respond after receiving the plain Authentication Reject, which aligns with the expected secure behavior defined by 3GPP. The UE did not proceed with any further communication, thereby minimizing the risk of information leakage or susceptibility to replay or downgrade attacks at this early, unauthenticated stage. Based on this analysis, the UE's action was secure and compliant with the 5G standard. Secure
56	56	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00040602684020996094 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated the registration process by sending an initial registration request to the AMF, which is standard behavior during NAS communication in 5G standalone networks. The AMF, under tester 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 standard, messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are allowed to be sent in plain text, as encryption and integrity protection are only activated after successful authentication and key agreement. The UE, upon receiving the "Authentication Reject" message, did not respond further, which aligns with the expected behavior as specified by the standard: upon receiving an "Authentication Reject," the UE should abort the registration attempt and not proceed with further NAS signaling. This prevents the UE from engaging in potentially insecure communication or exposing itself to further attacks. Therefore, the UE's action—ceasing communication after receiving a plain "Authentication Reject" prior to security context establishment—was secure and compliant with 3GPP standards. Secure

57	57	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003440380096435547 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an "Authentication Reject" message sent in plain (unencrypted) form, before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE is required to ignore or silently discard any NAS messages that are received in plain (unencrypted) form after the initial registration request, unless they are part of the authentication procedure (e.g., Authentication Request). Since the "Authentication Reject" was sent in plain text before security context establishment, and the UE did not respond to this message, the UE's behavior aligns with the 3GPP security requirements. This is because responding to or acting upon unauthenticated and unprotected messages could expose the UE to security risks such as impersonation or denial-of-service attacks. Therefore, the UE's action in not responding to the plain "Authentication Reject" message is considered secure according to the 5G 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 5G standalone registration 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, before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should not accept or act upon security-critical NAS messages (such as Authentication Reject) received in plain text before the completion of the authentication and establishment of NAS security context. The UE's correct behavior, upon receiving an unauthenticated and unprotected Authentication Reject message before 5G-AKA completion, is to ignore the message and not respond, as this could be an attempt at a security attack (e.g., a fake AMF trying to prematurely terminate registration). In this test, the UE did not respond to the plain Authentication Reject message, which aligns with the 3GPP security requirements and demonstrates that the UE did not accept unauthenticated commands that could compromise its security. Therefore, the UE's action in this scenario was secure. Secure

59	59	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0002620220184326172 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under tester 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 standard, messages prior to the completion of 5G-AKA (including authentication reject) are not protected by NAS security, and the UE must be able to handle such messages securely. Specifically, the UE should not respond to an "Authentication Reject" received in plain text before security activation, as this could be an attempt by an attacker to prematurely terminate the authentication process or cause a denial of service. In this test, the UE did not respond to the plain "Authentication Reject" message, which aligns with the 3GPP security recommendations and demonstrates resilience against a potential security attack. Therefore, the UE's action in this scenario was secure. Secure
60	60	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003459453582763672 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated the NAS registration procedure by sending an Initial Registration Request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication and key agreement procedure was completed. According to 3GPP 5G security standards, specifically TS 33.501, before the completion of 5G-AKA, all NAS messages are sent in plain text because mutual authentication and ciphering have not yet been established. Upon receiving an Authentication Reject message in plain text before authentication, the UE is expected to treat this as a security-critical event, as such a message could be spoofed by an attacker. The standard mandates that the UE must not respond to an unauthenticated Authentication Reject message and should silently discard it, to prevent denial-of-service or downgrade attacks. In this test, the UE did not respond to the plain Authentication Reject message, which aligns with the security requirements of the 5G standard. Therefore, the UE's behavior was secure, as it correctly ignored a potentially malicious message that arrived before authentication was established. Secure

61	61	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0004100799560546875 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a registration reject message using a plain (unencrypted) NAS message, with 5GMM Cause 111 (protocol error, unspecified). The 5G-AKA authentication procedure had not yet been completed, which means that the security context (encryption and integrity protection for NAS messages) was not yet established. According to the 3GPP 5G standard (TS 24.501), before authentication and security mode command are completed, NAS messages—including registration reject—are permitted to be sent in plain text, as the UE and network have not yet exchanged keys to enable encryption. The UE, upon receiving the plain registration reject, did not respond further, which is compliant with the standard; the UE is expected to accept the reject and not proceed with further registration attempts unless conditions change. Therefore, the UE's actions—accepting a plain registration reject prior to security context establishment and not responding further—are in line with 3GPP security requirements and do not expose the UE to additional risk in this context. Secure
62	62	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 17.596633911132812 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.597079038619995 AMF to UE SACK (Ack=14, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a Service Request message to the AMF, indicating it was attempting to initiate or resume a session. In response, the AMF sent a Deregistration 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 security standards, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected to ensure confidentiality and integrity. The UE, upon receiving the protected Deregistration Accept message, did not respond further. This behavior is consistent with the 3GPP standard, as the Deregistration Accept message is a terminal message in the deregistration procedure, and the UE is expected to cease NAS communication upon receipt. The UE's actions—sending a Service Request after authentication, accepting a protected Deregistration Accept message, and not responding further—demonstrate adherence to the security requirements of the 5G standard, as the UE did not process or respond to any unprotected or suspicious messages after security was established. 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, the UE and AMF completed the 5G-AKA authentication process, after which the UE sent an authentication response to the AMF. The AMF then sent a Security Mode Command to the UE, which was protected using the negotiated cipher (128-5G-EA1) and integrity (128-5G-IA2) algorithms, with the security header indicating "integrity protected with new security context." This means that the NAS security context was established, and subsequent NAS messages should be protected accordingly. After receiving the Security Mode Command, the UE responded with a Deregistration Request (UE originating). According to 3GPP standards (TS 33.501 and TS 24.501), once the security context is established, all subsequent NAS messages from the UE, including the Deregistration Request, must be integrity protected and, if required, ciphered. The packet capture shows that the Deregistration Request was sent after the security context was established, which implies that the UE followed the correct sequence and security procedures as per the standard. There is no indication that the UE sent any unprotected or unencrypted NAS messages after security activation. Therefore, the UE's actions were in line with 3GPP security requirements for NAS message protection after 5G-AKA completion and security mode activation. 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, the UE initiated a Service Request message to the AMF, which is the expected behavior for requesting network services. The AMF responded with a Service Accept message, which, according to the packet capture, was sent as a "Protected" (i.e., integrity protected and/or ciphered) NAS message. However, the UE did not respond to this protected downlink message from the AMF. According to the 3GPP 5G standards, once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. The UE is expected to process protected messages from the AMF and respond accordingly. The fact that the UE did not respond to a properly protected Service Accept message indicates a failure to comply with the expected 5G security procedures. This lack of response could expose the UE to potential denial of service or session establishment issues, and it suggests that the UE may not be correctly handling protected NAS messages as required by the standard. Therefore, based on the observed behavior and the 3GPP security requirements, the UE's action in this scenario was insecure. Insecure

65	65	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.15958499908447266 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16092395782470703 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36401796340942383 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to protect subsequent NAS messages. However, the AMF then sent another "security mode command" message, this time protected with the newly established security context (using ciphering and integrity algorithms), which is not the expected sequence according to the 3GPP 5G NAS protocol. According to the standard, once the UE has accepted the security mode and sent "security mode complete," the security context is established and further security mode commands are not expected unless there is a change in the security context (such as a handover or re-authentication event). The UE, upon receiving this unexpected and potentially suspicious "security mode command," responded with a "security mode reject" message, citing an unspecified reason. This behavior aligns with the security principles outlined by 3GPP, as the UE is expected to reject protocol messages that do not follow the correct sequence or may indicate a replay or misconfiguration attack. By refusing to process an out-of-sequence security mode command, the UE helps to prevent potential security breaches, such as downgrade or replay attacks. Therefore, the UE's action was secure and in compliance with 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 to the AMF, indicating that the UE was ready for further NAS procedures. The AMF then responded with a Security Mode Command, which was properly protected (integrity protected with a new security context) and specified the use of 128-5G-EA1 for ciphering and 128-5G-IA2 for integrity protection, with the ABBA parameter set to 0322. Upon receiving this Security Mode Command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to 3GPP standards (TS 24.501), a UE is permitted to reject a Security Mode Command if it detects any issues with the security context, the algorithms proposed, or if it cannot process the command for other security-related reasons. Since the Security Mode Command was sent with the correct security header and after 5G-AKA, the UE's rejection—while unspecified—does not violate the standard and could indicate that the UE detected a potential security anomaly or inconsistency. The UE did not proceed with insecure communication and instead halted the security procedure, which is a secure and conservative action as per 3GPP guidelines, especially in a test or potentially adversarial environment. Therefore, the UE's behavior aligns with secure practices as defined by the 5G standard. Secure

67	67	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.8137481212615967 UE to AMF UplinkNASTransport, Service request 0.8142230510711167 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Unknown) 1.0217480659484863 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes a secure context for NAS message protection), the UE sent a Service Request to the AMF. The AMF, under test control, responded with a protected GMM Status message carrying a 5GMM Cause value of 98. According to 3GPP TS 24.501, a GMM Status message with cause 98 ("Message type not compatible with the protocol state") is used to indicate that the received message type is unexpected in the current protocol state. Upon receiving this, the UE responded with its own 5GMM Status message, echoing the same cause. This behavior aligns with the 3GPP standard, which specifies that the UE should respond with a Status message when it receives a protected NAS message with an invalid or unexpected message type or cause in the current state. Since all NAS messages were protected (as required after 5G-AKA completion), and the UE did not process or act upon an invalid message but instead reported the protocol error as specified, the UE's actions were in accordance with the 5G security requirements and protocol robustness guidelines. Therefore, the UE's behavior in this interaction was 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, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a Service Request, which is a standard procedure to resume or establish a session with the network. The AMF responded with a Configuration Update Command, which, according to the packet capture, was sent as a protected message with integrity protection enabled (Security header: Integrity protected (1)). The UE then replied with a Configuration Update Complete message, indicating it properly processed the configuration update. The packet capture also shows that the UE sent this response as an UplinkNASTransport message, which is expected behavior. Since the 5G-AKA was completed prior to these exchanges, the security context (including keys for integrity and ciphering) should have been established, ensuring that subsequent NAS messages are protected according to 3GPP standards. The Configuration Update Command from the AMF was integrity protected, and the UE responded as expected, without exposing any sensitive information or violating the security procedures. Therefore, based on the sequence of events and the protection applied to the messages, the UE's actions align with the 3GPP 5G security requirements, and there is no indication of insecure behavior in the communication. Secure

69	69	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3100 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11985111236572266 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12013506889343262 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3252840042114258 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was integrity protected and indicated the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm. The security header specified that the message was integrity protected with a new security context. Upon receiving this, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G security standards (TS 33.501), it is generally considered insecure to accept a security context that does not provide confidentiality protection (i.e., uses the null ciphering algorithm 5G-EA0) unless under specific, controlled circumstances (such as emergency services or regulatory requirements). The UE's action to reject the Security Mode Command when only integrity protection (and no ciphering) was offered aligns with the security principles of 5G, which aim to prevent unencrypted user data transmission and protect against downgrade attacks. Therefore, the UE's behavior demonstrates adherence to 3GPP security requirements by refusing to proceed with insecure security parameters. Secure

70	70	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.547684907913208 UE to AMF UplinkNASTransport, Registration complete 0.5478739738464355 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration and security procedures had been completed. Subsequently, the AMF sent a "Security Mode Command" message to the UE, which was protected using integrity protection and ciphering with a new security context, as indicated by the security header (type 4). The ciphering algorithm selected was 5G-EA0 (null ciphering), meaning no encryption was applied, while the integrity algorithm was 128-5G-IA2, ensuring the message's integrity. Notably, the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard, after the security context is established and the Security Mode Command is received, the UE is expected to respond with a Security Mode Complete message if it accepts the proposed algorithms and context. The absence of a response from the UE suggests that it either rejected the null ciphering algorithm (5G-EA0) or failed to process the command, which is a secure behavior because the use of 5G-EA0 (null ciphering) is generally discouraged except in specific, controlled scenarios. The 3GPP standard recommends that UEs should not accept null ciphering unless explicitly allowed by operator policy, to prevent unencrypted user data transmission. Therefore, by not responding to the Security Mode Command that proposed null ciphering, the UE demonstrated secure behavior in line with 3GPP security recommendations. Secure

71	71	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0332 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 4.62968111038208 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 4.630121946334839 AMF to UE SACK (Ack=10, Arwnd=106361) , DownlinkNASTransport, Configuration update command 4.6305460929870605 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as NAS security should be established after authentication. The AMF then responded with a Security Mode Command, which was both integrity protected and ciphered, using cipher algorithm 128-5G-EA3 and integrity algorithm 5G-IA0 (null). According to the 3GPP 5G standard (TS 24.501), after 5G-AKA, the UE should accept the Security Mode Command if the parameters are acceptable and respond with a Security Mode Complete message. However, in this test, the UE did not respond to the Security Mode Command. The use of 5G-IA0 (null) for integrity protection means that the message is not integrity protected, which is generally not recommended except in very specific, controlled scenarios (e.g., for emergency services or as a fallback). The UE's lack of response can be interpreted as a refusal to proceed with insecure parameters, which aligns with 3GPP security recommendations that the UE should reject or not respond to security procedures that do not provide adequate protection (such as null integrity). Therefore, the UE's action of not responding to a Security Mode Command with null integrity protection is secure and compliant with the 5G standard, as it avoids establishing a session with insufficient security. Secure

72	72	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3300 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 6.590965032577515 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.591464042663574 AMF to UE SACK (Ack=25, Arwnd=106401) , DownlinkNASTransport, Configuration update command 6.5918920040130615 AMF to UE DownlinkNASTransport, Security mode command 6.7950029373168945 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message, and the AMF responded with a Security Mode Command message that was integrity protected and indicated the use of ciphering and integrity algorithms (5G-EA5 and 128-5G-IA2) with a new security context. Upon receiving this Security Mode Command, the UE responded with a Security Mode Reject message, specifying the cause as "Security mode rejected, unspecified." According to the 3GPP 5G standard, after 5G-AKA, the UE is expected to accept the Security Mode Command if the parameters (algorithms, ABBA value, etc.) are supported and valid. However, the UE is also required to reject the Security Mode Command if it detects any inconsistency, unsupported algorithms, or any security anomaly (such as an invalid security context or a mismatch in negotiated parameters). Since the Security Mode Reject cause is "unspecified," it is not clear from the UE's perspective what the exact issue was, but the fact that the UE did not proceed with potentially insecure or unsupported security parameters and instead halted the procedure by rejecting the command is a secure behavior. This prevents the UE from operating under potentially compromised or misconfigured security settings, which aligns with the security principles of the 3GPP standard. Therefore, the UE's action in this interaction can be considered secure. Secure

73	73	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1599750518798828 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602010726928711 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3605461120605469 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security algorithms and the establishment of a new security context. Unexpectedly, the AMF then sent another "security mode command" to the UE, this time protected with integrity but specifying the ciphering algorithm 5G-EA0 (null encryption) and integrity algorithm 128-5G-IA2, with the security header indicating integrity protection with the new security context. Upon receiving this, the UE responded with a "security mode reject" message, indicating that it rejected the security mode command for an unspecified reason. According to the 3GPP 5G standards (TS 24.501), after the security context is established and confirmed by "security mode complete," the AMF should not send a new "security mode command" unless there is a valid reason, such as a change in security parameters. Furthermore, the use of 5G-EA0 (null encryption) is only allowed under specific, controlled circumstances (e.g., emergency services or regulatory requirements), and the UE is permitted—and expected—to reject a security mode command that attempts to downgrade ciphering to null encryption in normal operation. The UE's rejection of the security mode command that requested null encryption is therefore consistent with the security requirements of the 5G standard, as it prevents potential downgrade attacks and ensures the confidentiality of user data. Based on this analysis, the UE acted securely and in accordance with 3GPP specifications. Secure

74	74	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03b3 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11993098258972168 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12021493911743164 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3277699947357178 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, indicating that mutual authentication was achieved and a security context could be established. The AMF then sent a Security Mode Command to the UE, which was integrity protected and indicated the use of ciphering algorithm 128-5G-EA3 and integrity algorithm 128-5G-IA2, with the security header showing "integrity protected with new security context." Upon receiving this command, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the reason. According to the 3GPP 5G standard (TS 24.501), a UE is permitted to reject a Security Mode Command if it detects issues such as unsupported algorithms, invalid parameters, or inconsistencies in the security context. The use of the "unspecified" cause suggests the UE detected an anomaly or could not process the command securely, and thus refused to proceed with establishing security based on the parameters provided. This behavior is in line with the security principles of 5G, which prioritize the integrity and confidentiality of communications and allow the UE to halt the procedure if security cannot be assured. Therefore, the UE's action to reject the Security Mode Command under these circumstances is considered secure and compliant with the standard, as it prevents the establishment of a potentially insecure connection. Secure

75	75	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0392 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.4745960235595703 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4750940799713135 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.47630810737609863 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, indicating that it was ready for further NAS procedures. The AMF then responded with a Security Mode Command message, which was sent as a protected message using the negotiated cipher (5G-EA5) and integrity (128-5G-IA1) algorithms, with the security header indicating "Integrity protected with new security context (3)." However, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, after the Security Mode Command is received, the UE is expected to verify the integrity of the message, apply the new security context, and respond with a Security Mode Complete message if the command is valid. The absence of any response from the UE means it did not acknowledge or accept the new security context, nor did it proceed with further protected NAS communication. This lack of response is not compliant with the standard, as it leaves the security procedure incomplete and could result in a denial of service or a security deadlock. Therefore, the action taken by the UE—failing to respond to a valid, protected Security Mode Command after 5G-AKA—was insecure, as it did not fulfill the required security handshake and left the communication in an indeterminate state. 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 replied with an identity request asking for the SUCI (Subscription Concealed Identifier) in plain (unencrypted) NAS signaling. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet activated. According to 3GPP standards (TS 33.501), the SUCI is a privacy-protected identifier designed to be sent only in plain text before NAS security is established, but it is also expected that the network should not request the SUCI after authentication has started, especially not after receiving an authentication response, as this could expose the UE to privacy risks if the SUCI is requested in plain text at an inappropriate stage. In this test, the UE did not respond to the AMF's identity request for the SUCI sent in plain text after authentication had begun. This behavior aligns with the security principle of not exposing the SUCI unnecessarily, especially after the authentication process is underway and before NAS security is established. By refusing to send the SUCI in this context, the UE protected the subscriber's privacy and adhered to the intent of the 3GPP security guidelines. Therefore, the UE's action in this scenario was secure. Secure

77	77	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0004799365997314453 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20071196556091309 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. In response, the AMF sent an identity request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. At this point in the NAS communication, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (integrity and encryption) had not been established, and all messages were exchanged in plain (unencrypted) form. The UE responded to the identity request by providing an identity response containing the SUCI. According to the 3GPP 5G standard, the SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) from exposure, even when transmitted over an unprotected channel before authentication and security activation. The SUCI is a concealed, pseudonymized version of the SUPI, generated using public key cryptography, and is intended to be sent in the clear during the initial registration phase. Therefore, the UE's action of providing the SUCI in response to an unprotected identity request prior to the completion of 5G-AKA is compliant with the 3GPP standard and does not expose sensitive subscriber information. Based on this, the UE's behavior in this scenario is considered 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 negotiated security algorithms and the establishment of a new security context. However, the AMF then sent another "security mode command" message, which was integrity protected but used the null ciphering algorithm (5G-EA0), meaning no encryption was applied to the messages. The UE responded to this with a "security mode reject" message, indicating a rejection of the security mode command for an unspecified reason. According to the 3GPP 5G security standards, once a security context is established and the security mode is completed, the UE expects all subsequent NAS messages to be both integrity protected and ciphered, unless there is a justified exception. The use of the null ciphering algorithm (5G-EA0) after security context establishment is generally not permitted, as it exposes user data and signaling to potential interception and manipulation. The UE's rejection of the security mode command that proposed null encryption aligns with the 3GPP security requirements, as it prevents the downgrading of security and protects the integrity and confidentiality of its communication. Therefore, the UE's action was secure and in compliance with the 5G standard. Secure

79	79	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1600358486175537 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16031789779663086 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36404991149902344 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after successfully completing the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command to the UE, specifying the use of the 5G-EA0 (null) ciphering algorithm (meaning no encryption) and the 128-5G-IA2 integrity algorithm, with the security header indicating integrity protection with a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, citing "Security mode rejected, unspecified" as the reason. According to the 3GPP 5G standard, after authentication, the UE should only accept security mode commands that provide both integrity and confidentiality protection, except in specific cases such as emergency services or certain network procedures. The use of 5G-EA0 (null encryption) is generally not permitted for normal user traffic, as it would leave the communication unencrypted and vulnerable to interception. By rejecting the security mode command that proposed null encryption, the UE correctly enforced the standard's security requirements, ensuring that its communications would not proceed without proper encryption. Therefore, the UE's action was secure and in compliance with 3GPP specifications. Secure
80	80	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.7228279113769531 UE to AMF UplinkNASTransport, Service request 0.723160982131958 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.9268310070037842 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a standard step for requesting network services. The AMF, under test control, responded with a Configuration Update Command message that was integrity protected and used a new security context, indicating that NAS security had been properly established as per 3GPP requirements. Upon receiving this message, the UE replied with a 5GMM Status message indicating "Message type not compatible with the protocol state." This response suggests that the UE detected the Configuration Update Command as unexpected or invalid in its current protocol state, and therefore did not process it further. According to 3GPP standards, the UE is required to check the validity and compatibility of received NAS messages with its current state, and to respond with a status message if an incompatible message is received. This behavior is a security feature designed to prevent protocol confusion or exploitation by malicious actors. The UE's action demonstrates that it correctly enforced protocol state checks and did not process an unexpected or potentially malicious message, which aligns with the security requirements of the 5G standard. Therefore, the UE's behavior in this interaction was secure. Secure

81	81	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 2222 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.1596660614013672 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1599440574645996 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then replied with a Security Mode Command. Notably, the Security Mode Command from the AMF specified the use of null algorithms for both ciphering (5G-EA0) and integrity protection (5G-IA0), meaning that no encryption or integrity protection would be applied to subsequent NAS messages. The security header indicated "integrity protected (1)", but with IA0 selected, this does not provide real protection. The UE, upon receiving this command, did not respond. According to the 3GPP 5G standard, the use of null algorithms is only permitted under specific, controlled circumstances (such as emergency services or when explicitly allowed by the operator's policy). In normal operation, the UE is expected to reject or not respond to a Security Mode Command that requests null algorithms, as accepting it would leave NAS signaling unprotected and vulnerable to interception or tampering. The UE's lack of response in this case aligns with secure behavior as defined by the standard, as it avoids establishing an insecure NAS security context. Therefore, the UE's action 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 the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then issued a Security Mode Command. The Security Mode Command specified the use of ciphering algorithm 128-5G-EA3 and the null integrity algorithm 5G-IA0, 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 an unspecified reason for rejection. According to the 3GPP 5G security standards (TS 33.501), integrity protection is mandatory for NAS signaling, and the use of the null integrity algorithm (5G-IA0) is only permitted under very limited circumstances (e.g., for emergency services or specific regulatory requirements). In normal operation, the UE is expected to reject any security mode command that requests null integrity protection, as this would leave the signaling vulnerable to tampering and attacks. The UE's action to reject the security mode command when asked to use 5G-IA0 aligns with the security requirements of the standard, as it prevents the establishment of a weak or insecure security context. Therefore, the UE's behavior in this interaction was secure and compliant with 3GPP specifications. 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, the 5G-AKA authentication procedure was completed, establishing the necessary security context for subsequent NAS message protection. The UE then sent a Service Request to the AMF, which is a typical step to request access to network services. The AMF responded with a Service Accept message, which was sent as a protected (i.e., integrity protected and/or ciphered) NAS message, as indicated in the test summary and packet capture. However, after receiving this protected Service Accept message, the UE did not provide any response. According to the 3GPP 5G standard, after the security context is established via 5G-AKA, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, ciphered. The UE is expected to process protected NAS messages and respond appropriately. The lack of response from the UE after receiving a protected Service Accept message suggests that the UE either failed to process the message or did not recognize it as valid, which could indicate a security implementation issue or a failure to comply with the expected protocol behavior. This lack of response could expose the UE to denial of service or other vulnerabilities if it cannot handle protected messages correctly after authentication. Therefore, based on the 3GPP standard and the observed behavior, the UE's action in this scenario is considered insecure. Insecure

84	84	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0083 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11982488632202148 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12009406089782715 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3228750228881836 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was protected using the negotiated ciphering (128-5G-EA2) and integrity (128-5G-IA2) algorithms, and indicated the use of a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, the UE is expected to accept the Security Mode Command if the parameters (algorithms, ABBA, etc.) are valid and consistent with the negotiated security context. A Security Mode Reject is only expected in cases where the UE detects an issue, such as an unsupported algorithm, mismatched security context, or integrity failure. In this case, the rejection cause is "unspecified," which does not provide a clear reason for the rejection. However, since the Security Mode Command was properly protected and the 5G-AKA was completed, the UE's refusal to proceed without a specific, standards-based reason could indicate overly cautious or non-compliant behavior, but it does not directly expose the UE to security risks. The UE did not proceed with unprotected communication or accept potentially insecure parameters, which aligns with a secure posture, even if the rejection was not fully explained. Therefore, the UE's action can be considered secure, as it did not compromise the integrity or confidentiality of the communication, despite the lack of a specific rejection reason. 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 the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the negotiated security parameters. However, the AMF then sent another "security mode command" message, this time protected, specifying the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, with the security header indicating "integrity protected with new security context." Upon receiving this, the UE responded with a "security mode reject" message, citing an unspecified reason for rejection. According to the 3GPP 5G security standards, after authentication, the UE and network must agree on security algorithms that provide confidentiality and integrity protection; the use of null algorithms (EA0/IA0) is only allowed in very limited, controlled scenarios (such as emergency services or specific test cases), and generally, the UE should reject any attempt to establish a security context with null algorithms if not explicitly permitted. The UE's action to reject the security mode command when null algorithms were proposed aligns with the 3GPP security requirements, as accepting such parameters would leave user data and signaling unprotected, exposing the UE to potential security threats. Therefore, the UE's behavior demonstrates adherence to the standard and a secure response to a potentially insecure configuration. Secure

86	86	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered (2) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.15096688270568848 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15124177932739258 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.35789990425109863 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the negotiated security algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity) and was ready to establish a protected NAS security context. However, the AMF, under test control, responded with another "security mode command" message, which is not expected behavior according to the 3GPP 5G standard (TS 24.501). The UE then sent another "security mode complete" message in response. According to the 3GPP standard, after the UE sends "security mode complete," the NAS security context is established, and further "security mode command" messages should not be sent unless the context is re-initialized or updated. The UE, upon receiving a second "security mode command," should have rejected it or ignored it, as accepting and responding to repeated or unexpected security mode commands can open the door to replay or downgrade attacks. By sending another "security mode complete" in response to an unexpected "security mode command," the UE did not adhere to the expected security procedures, potentially exposing itself to security vulnerabilities. Therefore, the UE's action in this scenario was **not secure** according to 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 the successful completion of 5G-AKA authentication and security setup, the UE sent a Service Request to the AMF. In response, the AMF sent a Deregistration Request message that was integrity protected and ciphered, indicating that the NAS security context was active. Upon receiving this protected deregistration request, the UE responded with a 5GMM Status message indicating "Invalid mandatory information," and then re-initiated the registration process by sending an InitialUEMessage and another Service Request. According to the 3GPP 5G standard (TS 24.501), when the UE receives a NAS message that is integrity protected and ciphered but contains invalid or unrecognized mandatory information elements, the correct behavior is for the UE to send a 5GMM Status message with the appropriate cause value ("invalid mandatory information"). This ensures that the UE does not process potentially malformed or malicious messages, thus maintaining the integrity and security of the NAS protocol. The UE did not accept or process the deregistration request, but instead reported the error and attempted to re-establish service, which aligns with the standard's requirements for secure handling of protected NAS messages. Therefore, the UE's actions demonstrate adherence to the 3GPP security requirements and proper error handling in the face of unexpected or invalid protected messages. Secure
88	88	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.1599421501159668 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1602020263671875 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request 0.36409711837768555 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, but the 5G-AKA authentication procedure was not yet completed. Subsequently, the AMF sent an identity request for the SUCI (Subscription Concealed Identifier) to the UE in plain (unencrypted) NAS, and the UE responded with an identity response. According to the 3GPP 5G security standard, the UE is required to respond to identity requests from the network even when NAS security (encryption and integrity protection) is not yet established, particularly before the completion of 5G-AKA. However, the UE must never send the cleartext SUPI (Subscription Permanent Identifier); instead, it should only send the SUCI, which is a privacy-preserving, encrypted version of the SUPI, specifically designed to protect the subscriber's identity even over unprotected channels. In this case, the UE correctly responded with the SUCI, not the SUPI, in the identity response. Therefore, the UE's actions were in line with 3GPP security requirements, as it did not expose sensitive information before NAS security was established. The UE's behavior was secure given the context and the standards. Secure

89	89	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.12005400657653809 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12025594711303711 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request 0.3216700553894043 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS steps and sent an authentication response to the AMF, but the 5G-AKA authentication procedure was not yet completed. Immediately after, the AMF sent an identity request for the SUCI (Subscription Concealed Identifier), and the UE responded with an identity response. Importantly, the AMF sent the identity request message in plain (unencrypted) form, which is expected since the security context (encryption and integrity protection) is not established until after the successful completion of 5G-AKA. According to the 3GPP 5G standard, prior to the completion of 5G-AKA, all NAS messages—including identity requests and responses—are permitted to be sent in plain text, as encryption keys are not yet available. The SUCI itself is a privacy-preserving identifier designed to be sent in the clear, as it does not reveal the permanent subscriber identity (SUPI) and is constructed to protect user privacy even over unprotected channels. Therefore, the UE's action of responding to a plain identity request with a SUCI in the identity response before the completion of 5G-AKA is compliant with the 3GPP standard and does not constitute a security weakness. The UE did not expose any sensitive information and followed the expected protocol behavior. Secure
90	90	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.11975502967834473 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999011039733887 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request 0.3266119956970215 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, but the 5G-AKA authentication process was not yet completed. Subsequently, the AMF sent an identity request to the UE, specifically requesting the SUCI (Subscription Concealed Identifier), and this message was sent in plain (unencrypted) form. The UE responded with an identity response, also in plain text, as encryption had not yet been established due to the incomplete 5G-AKA process. According to the 3GPP 5G security standards, prior to the completion of 5G-AKA, NAS messages—including identity requests and responses—are allowed to be sent in plain text, as mutual authentication and key establishment have not yet occurred. The SUCI is designed to protect the subscriber's permanent identity (SUPI) even when transmitted in the clear, as it is a concealed, privacy-preserving identifier. Therefore, the UE's action of responding with the SUCI in plain text before security activation is compliant with 3GPP standards and does not expose sensitive information. Based on this, the UE's behavior in this interaction is considered secure according to the 5G standard. Secure

91	91	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7701981067657471 UE to AMF UplinkNASTransport, Service request 0.7708969116210938 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal UE) 0.9781770706176758 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a typical step to request access to network services. In response, the AMF (under tester control) sent a deregistration request, indicating that the UE is considered "Illegal" and should be deregistered. Notably, this deregistration request was sent as a protected NAS message, meaning it was both integrity protected and ciphered, as required after 5G-AKA completion. The UE then responded with a 5GMM status message indicating "Invalid mandatory information," which suggests that the UE detected an issue with the content or structure of the deregistration request. According to the 3GPP 5G standards, after security activation, the UE must only accept and process NAS messages that are integrity protected and ciphered; if a protected message contains invalid or missing mandatory information, the UE should respond with a status message indicating the error, as was done here. Therefore, the UE's actions—refusing to process an invalid deregistration request and reporting the error—are in line with the security requirements and expected behavior defined by 3GPP. The UE did not process or accept an unprotected or malformed message and maintained the integrity of the secure communication channel. Based on this analysis, the UE's actions were secure. 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 security test scenario, the 5G User Equipment (UE) first completed the 5G-AKA authentication and key agreement procedure, ensuring that both the UE and the Access and Mobility Management Function (AMF) established a secure context for subsequent NAS (Non-Access Stratum) communication. After authentication, the UE sent a service request to the AMF, which then responded with a deregistration request message. Importantly, the deregistration request from the AMF was sent as a protected message, with both integrity protection and ciphering applied, as indicated by the security header (value 2). Upon receiving this protected deregistration request, the UE responded with a deregistration accept message, thereby following the expected protocol behavior. According to the 3GPP 5G standards, after the successful completion of 5G-AKA, all subsequent NAS messages, especially those that can impact the UE's registration state (such as deregistration), must be integrity protected and ciphered to prevent security breaches like spoofing or replay attacks. The UE, in this case, only accepted and responded to a deregistration request that was properly protected, indicating that it adhered to the security requirements outlined by 3GPP. Therefore, the actions taken by the UE were secure and in compliance with the standard. 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 this 5G standalone security test, the User Equipment (UE) and Access and Mobility Management Function (AMF) completed the 5G-AKA authentication procedure, establishing a security context for subsequent NAS message protection. The UE then sent a "security mode complete" message, indicating it had accepted the security parameters previously negotiated. However, the AMF subsequently issued another "security mode command" message, this time protected and specifying ciphering with 5G-EA4 and integrity protection with 5G-IA0 (null integrity). Upon receiving this, the UE responded with a "security mode reject" message, citing a "UE security capabilities mismatch." According to the 3GPP 5G standards, the UE is required to verify that the security algorithms proposed by the network are supported and acceptable. If there is a mismatch, especially if the network proposes an integrity algorithm that is not supported or is insecure (such as 5G-IA0, which provides no integrity protection), the UE must reject the security mode command to prevent potential security vulnerabilities. The UE's action to reject the security mode command due to a security capabilities mismatch aligns with the 3GPP standard's intent to ensure that only mutually supported and secure algorithms are used, thereby protecting the integrity and confidentiality of NAS signaling. Therefore, the UE's behavior in this scenario was secure and compliant with the 5G standard. Secure
94	94	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00028896331787109375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20491886138916016 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with 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, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established, and all messages exchanged—including the identity request and response—were sent in plain (unencrypted) form. According to the 3GPP 5G standard, it is expected and required that the UE responds to an identity request with the SUCI, which is a privacy-preserving, concealed version of the permanent subscriber identity (SUPI). The SUCI is specifically designed to be sent over an unprotected channel before NAS security is activated, to prevent exposure of the SUPI and protect user privacy. Therefore, the UE's action—responding with the SUCI in plain text prior to the completion of 5G-AKA—is in full compliance with the 3GPP standard and does not expose sensitive information. The UE did not send the SUPI or any unprotected sensitive identifier, and thus maintained the expected level of security for this phase of registration. 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 5G-AKA authentication (which establishes security context for NAS message protection), the UE sent a Service Request to the AMF. In response, the AMF sent a Deregistration Request (UE terminated) as a downlink NAS message, which was integrity protected and ciphered, indicating that NAS security was active. The UE then replied with a Deregistration Accept (UE terminated), also protected under the established security context. According to 3GPP standards, after 5G-AKA, all subsequent NAS messages must be integrity protected and ciphered, which was observed in this interaction. Although the Deregistration Request from the AMF was unexpected (as it is not a typical response to a Service Request and is noted as "Message type not compatible with the protocol state"), the UE correctly processed the protected message and responded as specified by the protocol—by sending a Deregistration Accept. The UE did not process or respond to any unprotected or suspicious messages, and it adhered to the security requirements by only accepting and responding to properly protected NAS messages. Therefore, the UE's actions were secure according to the 3GPP 5G standard, as it maintained the integrity and confidentiality of NAS signaling and followed protocol procedures even in the face of unexpected but properly protected messages. Secure
96	96	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.039906978607177734 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04016995429992676 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2424759864807129 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and responded to an identity request from the AMF by sending an identity response. After this, the AMF (under tester control) sent another identity request for the SUCI (Subscription Concealed Identifier), and the UE responded again with an identity response. Importantly, the 5G-AKA authentication procedure had not yet been completed, so NAS security (encryption and integrity protection) was not yet established; thus, the identity request from the AMF was sent in plain text, and the UE's response was also unprotected. According to the 3GPP 5G standard, it is expected that certain initial NAS messages, including identity requests and responses, may be sent in the clear before authentication and key agreement are completed, as the network needs to identify the UE before establishing a secure channel. However, the UE must ensure that it only provides the SUCI (which is a privacy-preserving, encrypted form of the SUPI) and never the cleartext SUPI (IMSI) before security is established. In this interaction, the UE responded with the SUCI, which is specifically designed to protect the subscriber's permanent identity even when sent without NAS security. Therefore, the UE's actions were in line with the 3GPP security requirements, as it did not expose sensitive information in the clear and followed the expected protocol behavior. Secure

97	97	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03965497016906738 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0398409366607666 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24122309684753418 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS steps and 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 responded again with 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 the 3GPP 5G standard, the UE is required to protect its permanent identifier (SUPI) and should only send the SUCI, which is a privacy-preserving, concealed version of the SUPI, in plain NAS messages prior to security activation. The SUCI is specifically designed to be transmitted before security is established, as it does not reveal the permanent identity of the subscriber. Based on the packet capture and the summary, the UE responded to the AMF's plain identity request with the SUCI, which aligns with the 3GPP security requirements. Therefore, the UE's actions were in accordance with the 5G standard and did not expose sensitive information. Secure
98	98	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.798314094543457 UE to AMF UplinkNASTransport, Service request 0.7985830307006836 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command 1.0063400268554688 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a Service Request to the AMF, which is a standard step to resume or establish a session. The AMF then responded with a Configuration Update Command, sent as a protected (integrity-protected) NAS message with a new security context, indicating that the security procedures were properly established and the message was secured as per 3GPP requirements. Upon receiving this message, the UE replied with a 5GMM Status message indicating "Message type not compatible with the protocol state." This response from the UE suggests that it detected an unexpected or out-of-sequence message from the AMF, and rather than processing it blindly, the UE flagged the protocol error as specified in the 3GPP standards (TS 24.501, section 8.2.28). This behavior demonstrates that the UE is correctly enforcing protocol state checks and is not accepting potentially invalid or malicious messages, even when they are integrity protected. By refusing to process a message that is not compatible with its current protocol state and reporting the error, the UE is adhering to the security and robustness requirements of the 5G standard. Therefore, the UE's actions in this scenario are secure and compliant with 3GPP specifications. Secure

99	99	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.5202081203460693 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5204141139984131 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test, after completing the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. The AMF then responded with a Downlink NAS Transport message containing a Service Accept, which was sent as a protected (i.e., integrity protected and/or ciphered) message. However, the UE did not respond to this protected downlink message from the AMF. According to the 3GPP 5G standard, after successful 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered to ensure confidentiality and authenticity. The fact that the UE did not respond to a properly protected Service Accept message from the AMF suggests that the UE either failed to process the protected message or did not recognize it as valid, which is not compliant with the expected behavior outlined in the 3GPP standards. The UE should have been able to process and respond to protected NAS messages after 5G-AKA completion. Therefore, based on the observed behavior, the UE's action is considered insecure as it failed to handle protected NAS messages as required by the 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 successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context was established and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered). Following this, the AMF sent a protected "GMM Status" message with a 5GMM cause value of 92, which corresponds to "Insufficient user-plane resources for the PDU session." The UE, upon receiving this protected status message, did not respond. According to the 3GPP 5G standards (TS 24.501), after the security context is established, the UE is expected to process protected NAS messages and only respond to certain status messages if required by the protocol. Specifically, for a GMM Status message with cause 92, the standard does not mandate a response from the UE; it is an informational message indicating a resource issue, not requiring UE action. The fact that the UE did not respond to this protected status message is therefore compliant with the standard and does not indicate any security weakness. The UE maintained the integrity and confidentiality of its communication by only sending and accepting protected messages after 5G-AKA, and it did not leak any information or behave unexpectedly in response to the status message. Based on this analysis, the UE's actions were secure and in accordance with 3GPP requirements. Secure

101	101	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 4.873120069503784 UE to AMF SACK (Ack=7, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 4.873471021652222 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is a typical step in establishing a PDU session. In response, the AMF sent a Security Mode Command message to the UE, which was correctly protected using the negotiated ciphering (128-5G-EA3) and integrity (128-5G-IA2) algorithms, and marked as "Integrity protected with new security context" as per 3GPP standards. However, the UE did not respond to this Security Mode Command. According to the 3GPP 5G NAS protocol, upon receiving a Security Mode Command that is properly protected and after successful authentication, the UE is required to process the command, activate the indicated security algorithms, and send a Security Mode Complete message back to the AMF. The lack of any response from the UE is a deviation from the expected secure behavior, as it leaves the security context unconfirmed and the session potentially vulnerable. This failure to respond could indicate a flaw in the UE's NAS security handling, as it neither confirms the establishment of the security context nor continues with the secure session setup. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure. Insecure

102	102	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7492289543151855 UE to AMF UplinkNASTransport, Service request 0.749459981918335 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9532349109649658 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the described test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Service Request to the AMF, which then responded with a Security Mode Command. 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 providing no actual encryption or integrity protection. The security header indicated "Integrity protected with new security context," but since the algorithms were null, no real protection was applied. Upon receiving this, the UE responded with a 5GMM Status message indicating "Invalid mandatory information," suggesting that the UE detected an issue with the Security Mode Command, likely due to the use of null algorithms after authentication. According to the 3GPP 5G standard, after the establishment of a security context (post-5G-AKA), the use of null algorithms for either ciphering or integrity is not permitted for normal operation, as this would leave NAS messages unprotected and vulnerable to interception or tampering. The UE's action to reject the Security Mode Command and report invalid mandatory information aligns with the standard's security requirements, as it prevents the establishment of an insecure communication session. Therefore, the UE acted securely by refusing to proceed with null security algorithms 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 security test, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending a Deregistration Request (UE terminated) message back to the UE. The Deregistration Request from the AMF was sent with a security header indicating that it was both integrity protected and ciphered, meaning it was encrypted and authenticated as per 3GPP 5G security standards. The UE, upon receiving this protected deregistration request, did not respond. According to 3GPP specifications, after receiving a properly protected Deregistration Request from the network, the UE is expected to process the request, initiate deregistration procedures, and typically send a Deregistration Accept message back to the AMF. The lack of response from the UE indicates that it did not follow the expected protocol behavior, which could lead to potential security or operational issues, such as the network being unaware of the UE's deregistration status. This deviation from the standard protocol flow suggests that the UE's action was not fully secure or compliant with 3GPP requirements, as it failed to properly acknowledge and process a legitimate, protected network command. Insecure

104	104	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5198929309844971 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5201320648193359 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (LADN not available) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was successfully completed, establishing a secure context for subsequent NAS communication between the UE and the AMF. After authentication, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. In response, the AMF sent a Deregistration Request (UE terminated), which was integrity protected and ciphered, as indicated by the security header (2), meaning the message was both encrypted and authenticated according to 3GPP standards. The UE, upon receiving this protected deregistration request, did not respond. According to 3GPP TS 24.501, when a UE receives a deregistration request that is properly protected (integrity protected and ciphered) after a valid 5G-AKA, the UE should process the request and deregister, typically responding with a deregistration accept message. The lack of response from the UE indicates that it did not process the deregistration request as specified by the standard. This behavior could be interpreted as insecure, as the UE failed to follow the expected protocol for secure deregistration, potentially leaving the session in an inconsistent or vulnerable state. Therefore, based on the 3GPP standard, the UE's action in this scenario was not secure. Insecure
105	105	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5608680248260498 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5614829063415527 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7653870582580566 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a UL NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a configuration update command as a downlink NAS message, which was marked as "Protected" and included a security header indicating that it was both integrity protected and ciphered (security header type 2). The UE then replied with a configuration update complete message, confirming receipt and processing of the configuration update command. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the communication. The packet capture confirms that the downlink message from the AMF was protected, and the UE responded appropriately with a configuration update complete message, indicating that it correctly processed the secured message. Since the UE only sent and responded to messages after security activation, and there is no indication of the UE sending or accepting unprotected NAS messages post-authentication, the UE's actions align with the security requirements of the 5G standard. Therefore, the UE's behavior in this interaction was secure. Secure

106	106	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.7586648464202881 UE to AMF UplinkNASTransport, Service request 0.7588739395141602 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9626758098602295 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using the negotiated ciphering (5G-EA4) and integrity (128-5G-IA3) algorithms, and marked with the security header type "Integrity protected with new security context (3)". 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 (TS 24.501), the UE is required to verify that the security algorithms proposed by the network are supported and match its own capabilities. If there is a mismatch, the UE must reject the security mode command to prevent the establishment of a security context with unsupported or potentially insecure algorithms. This behavior ensures that the UE does not operate under a security configuration that could compromise its integrity or confidentiality. Therefore, the UE's action to reject the security mode command due to a capabilities mismatch is compliant with the 3GPP standard and demonstrates secure behavior in this context. Secure
107	107	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.46604204177856445 UE to AMF UplinkNASTransport, Registration complete 0.466264009475708 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Restricted service area) 0.6700358390808105 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that it had finished the registration process. Immediately following this, the AMF sent a "Deregistration Request" message to the UE, which was integrity protected and ciphered, as indicated by the security header (2). The UE responded with a "Deregistration Accept" message, acknowledging the request. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The packet capture confirms that the deregistration request from the AMF was indeed protected, and the UE responded appropriately by sending a deregistration accept message. The UE did not process or respond to any unprotected or unexpected messages, and it followed the expected protocol behavior as per the standard. Therefore, the UE's actions were secure, as it only accepted and responded to protected messages after authentication, maintaining the integrity and confidentiality required by 3GPP specifications. Secure

108	108	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.5200989246368408 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5204448699951172 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7219538688659668 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes the security context for NAS message protection), the UE sent an Uplink NAS Transport message to the AMF, likely as part of a PDU session establishment request. The AMF then responded with a Configuration Update Command, which was correctly protected using integrity protection and a new security context, as indicated by the security header. Upon receiving this message, the UE replied with a 5GMM Status message, indicating "Message type not compatible with the protocol state." According to the 3GPP 5G NAS specifications (TS 24.501), if the UE receives a NAS message that is not compatible with its current protocol state, it should respond with a 5GMM Status message, as this is the standardized mechanism for error reporting and protocol robustness. The UE's action demonstrates adherence to the protocol by not processing an unexpected or out-of-sequence message, thereby preventing potential state confusion or security vulnerabilities. The UE also maintained the integrity and security of the communication by only responding after 5G-AKA completion and using the established security context. Therefore, the UE's behavior aligns with the 3GPP security requirements and protocol expectations for handling such scenarios. Secure
109	109	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.5209951400756836 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215010643005371 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Unknown) 0.7227599620819092 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes security context for NAS message protection), the UE sent an Uplink NAS Transport message to the AMF, which is a standard procedure for initiating further NAS procedures such as PDU session establishment. The AMF, under tester control, responded with a protected GMM Status message containing a 5GMM cause value of 98, which indicates "Message type not compatible with the protocol state" according to 3GPP TS 24.501. The UE, upon receiving this unexpected and protocol-incompatible GMM status message, replied with its own GMM Status message, explicitly indicating that the received message type was not compatible with the current protocol state. This behavior aligns with the 3GPP standard, which specifies that the UE should respond with a GMM Status message when it receives a NAS message that is not compatible with its current state, thereby providing feedback to the network and maintaining protocol integrity. The fact that the UE only responded with a status message and did not process or act upon the invalid command demonstrates that it did not deviate from the expected secure behavior as per 3GPP specifications. Therefore, based on the observed actions and adherence to the standard, the UE's response can be considered secure. Secure

110	110	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 101 UE provided: No response The packet capture during the test using wireshark is: 0.5881869792938232 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originating) 0.5883810520172119 AMF to UE SACK (Ack=6, Arwnd=106429) , DownlinkNASTransport, 5GMM status (Message not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that it had finished the registration process. Immediately following this, the AMF sent a protected (i.e., encrypted and integrity-protected) "5GMM Status" message to the UE with a 5GMM Cause value of 101, which corresponds to "Message not compatible with the protocol state" as per 3GPP TS 24.501. The UE did not respond to this status message. According to the 3GPP standard, after the registration procedure is complete, the UE is not expected to respond to a 5GMM Status message, especially if the cause indicates an unexpected or out-of-state message. The fact that the message from the AMF was protected confirms that the security context was established and that the UE only responded to legitimate, expected messages. By not responding to an unsolicited or protocol-incompatible status message, the UE avoided potential security pitfalls such as unnecessary information disclosure or protocol confusion. This behavior aligns with the 3GPP security guidelines, which recommend that UEs ignore or silently discard protected messages that are not compatible with the current protocol state. Therefore, the UE's action in this scenario was secure. Secure
111	111	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.7300009727478027 UE to AMF UplinkNASTransport, Service request 0.7302379608154297 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9340109825134277 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. The AMF responded with a Security Mode Command, which was integrity protected and indicated the use of ciphering algorithm 5G-EA5 and integrity algorithm 5G-IA0 (null integrity). The UE then rejected the Security Mode Command with the cause "UE security capabilities mismatch." According to the 3GPP 5G standard, the UE is required to verify that the security algorithms proposed by the network are within its declared capabilities and that integrity protection is not downgraded in a way that could compromise security. The use of 5G-IA0 (null integrity) is generally not recommended for user plane or NAS signaling, as it provides no integrity protection, and the UE is expected to reject such configurations if it does not support them or if it violates security policy. The UE's action to reject the Security Mode Command due to a security capabilities mismatch is compliant with the 3GPP standard and demonstrates that the UE is enforcing proper security checks to prevent potential downgrade attacks or misconfigurations. Therefore, the UE's behavior in this scenario is secure. Secure

112	112	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.7296979427337646 UE to AMF UplinkNASTransport, Service request 0.7299599647521973 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9337029457092285 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using the negotiated cipher (5G-EA5) and integrity (128-5G-IA2) algorithms, and indicated a new security context in the security header. Upon receiving this command, the UE replied with a Security Mode Reject message, citing a "UE security capabilities mismatch." According to the 3GPP 5G standard (TS 24.501), the UE is required to check whether the security algorithms proposed by the network are supported by its own capabilities, which were previously communicated during the registration or authentication phase. If there is a mismatch—meaning the AMF requests algorithms the UE does not support—the UE must reject the security mode command to prevent the establishment of an insecure or unsupported security context. This behavior is a critical security measure to avoid the use of weak or incompatible algorithms that could compromise the confidentiality or integrity of NAS signaling. Therefore, the UE's action to reject the security mode command due to a capabilities mismatch is in strict accordance with 3GPP security requirements and demonstrates secure behavior in this context. Secure

113	113	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 14.246875047683716 UE to AMF UplinkNASTransport, Service request 14.247098922729492 AMF to UE SACK (Ack=15, Arwnd=106496) , DownlinkNASTransport, Security mode command 14.454866886138916 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was properly protected using the negotiated ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms, and included a security header indicating "integrity protected with new security context." Upon receiving this message, the UE responded with a Security Mode Reject, specifying "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, a UE is expected to reject a Security Mode Command only if it detects an issue such as an unsupported algorithm, an integrity failure, or another security-related problem. Since the Security Mode Command was sent with appropriate protection and after successful authentication, the UE's rejection without a specified cause ("unspecified") may indicate either a security concern detected by the UE (such as a mismatch in context, replayed message, or internal error) or a non-compliant behavior if no real issue existed. However, from a security perspective, it is generally safer for a UE to reject a security procedure if it cannot guarantee the integrity or confidentiality of the session, even if the cause is unspecified, as this prevents potential exploitation. Therefore, the UE's action, while not fully transparent, aligns with a conservative security posture as recommended by 3GPP, prioritizing the protection of user data and signaling over continued connectivity in the face of uncertainty. 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, the 5G-AKA authentication procedure was completed first, which is a prerequisite for establishing NAS security between the User Equipment (UE) and the Access and Mobility Management Function (AMF). Following this, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request), and the AMF responded with a Configuration Update Command. The packet capture shows that the downlink Configuration Update Command from the AMF was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered, as per the 3GPP 5G NAS security specifications. The UE then responded with a Configuration Update Complete message, indicating that it processed the command successfully. According to 3GPP standards, after 5G-AKA is completed, all subsequent NAS messages should be protected by integrity and ciphering to ensure confidentiality and authenticity. The actions taken by the UE—processing only protected messages after security activation and responding appropriately—align with these security requirements. Therefore, based on the observed behavior and adherence to the 3GPP 5G security standard, the UE's actions in this interaction were secure. Secure

115	115	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 14.061744928359985 UE to AMF UplinkNASTransport, Service request 14.062045097351074 AMF to UE SACK (Ack=16, Arwnd=106496) , DownlinkNASTransport, Security mode command 14.26575493812561 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a Service Request to the AMF. The AMF responded with a Security Mode Command, which was sent as a protected message using the negotiated cipher (5G-EA4) and integrity (128-5G-IA3) algorithms, and with the security header indicating "Integrity protected with new security context (3)", as per 3GPP standards for establishing NAS security. However, upon receiving this Security Mode Command, the UE responded with a 5GMM status message indicating "Invalid mandatory information." According to 3GPP TS 24.501, after receiving a Security Mode Command that is properly protected and formatted, the UE is expected to process the command, activate the indicated security algorithms, and respond with a Security Mode Complete message. The UE should only send a 5GMM status message with "Invalid mandatory information" if the Security Mode Command is malformed or missing required information. Since the AMF (under test control) sent a standards-compliant, protected Security Mode Command, the UE's response suggests it either failed to correctly process a valid message or incorrectly identified it as invalid. This behavior is not compliant with 3GPP security procedures, as it may indicate improper handling of security context establishment or message validation, potentially exposing the UE to security vulnerabilities or interoperability issues. Therefore, based on the observed interaction and 3GPP requirements, the action taken by the UE was insecure. Insecure

116	116	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00d2 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.480457067489624 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4812970161437988 3 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.6844742298126221 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, which was followed by the AMF sending a Security Mode Command (SMC) message. The SMC from the AMF was protected, indicating that it was integrity protected and ciphered using the negotiated algorithms (128-5G-EA2 for ciphering and 128-5G-IA2 for integrity), and the security header indicated a new security context was being used. Upon receiving this SMC, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to 3GPP standards (TS 24.501), a UE is expected to accept the Security Mode Command if the parameters are valid and the message is correctly protected; otherwise, it may reject the command if it detects issues such as an unsupported algorithm, an invalid security context, or integrity/ciphering failures. However, in this case, the rejection cause is "unspecified," and there is no evidence from the trace that the SMC was malformed, used unsupported algorithms, or failed integrity checks. Since the SMC was protected and the algorithms are standard, the UE's rejection without a specific cause could indicate a failure to properly process a valid and secure message, which is not compliant with 3GPP expectations for secure operation. Therefore, the UE's action in this scenario is considered insecure, as it did not proceed with establishing a secure context despite all security prerequisites being met and did not provide a specific reason for the rejection, which could expose the network to denial-of-service or downgrade attacks if exploited. Insecure

117	117	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.5606789588928223 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5618300437927246 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a UL NAS Transport message to the AMF, which then responded with a Security Mode Command message. The Security Mode Command was correctly protected, as indicated by the use of integrity protection and ciphering with a new security context, using the specified cipher (5G-EA5) and integrity (128-5G-IA1) algorithms. However, the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard (TS 24.501), upon receiving a Security Mode Command that is properly protected and after successful authentication, the UE is required to process the command, activate the indicated security algorithms, and respond with a Security Mode Complete message. The lack of response from the UE is a deviation from the standard, as it leaves the security procedure incomplete and could potentially expose the session to risks if further communication occurs without proper security context establishment. Therefore, the UE's action in not responding to a valid, protected Security Mode Command is considered insecure according to the 5G standard. Insecure
118	118	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 6.6406471729278564 UE to AMF SACK (Ack=8, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 6.641204118728638 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Configuration update command 6.843037128448486 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending a Configuration Update Command. The packet capture indicates that the Configuration Update Command from the AMF was sent as a protected message, specifically with a security header indicating both integrity protection and ciphering (security header type 2). The UE then responded with a Configuration Update Complete message. According to the 3GPP 5G standards (TS 24.501), after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The UE's actions—accepting and responding to a protected Configuration Update Command—are in line with these requirements. The UE did not process any unprotected or insecure messages after the security context was established, and its response was appropriate and secure as per the standard. Therefore, the UE's actions in this interaction were secure. Secure

119	119	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.5208361148834229 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5222671031951904 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.7242951393127441 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an uplink NAS transport message to the AMF, which then responded with a Security Mode Command. The Security Mode Command from the AMF specified the use of the 5G-EA0 (null) ciphering algorithm (meaning no encryption) and the 128-5G-IA1 integrity algorithm, and was sent as a protected message with a new security context. Upon receiving this, the UE responded with a Security Mode Reject message, indicating that it rejected the security mode command for an unspecified reason. According to the 3GPP 5G standard, after authentication, the UE and the network must agree on security algorithms for both integrity and ciphering to ensure confidentiality and integrity of NAS signaling. The use of 5G-EA0 (null ciphering) is only permitted in very specific, controlled scenarios (such as emergency services or regulatory requirements), and generally, the UE is expected to reject the use of null ciphering in normal operation to prevent unencrypted communication. The UE's rejection of the security mode command that proposed null ciphering demonstrates adherence to security best practices as outlined by 3GPP, as it prevents the establishment of an insecure connection. Therefore, the UE's actions were secure and in compliance with the 5G standard. Secure
120	120	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.46767306327819824 UE to AMF UplinkNASTransport, Registration complete 0.46790289878845215 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this 5G standalone security test, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating the end of the registration process. Immediately following this, the AMF sent a "Deregistration Accept" message to the UE, which was protected (i.e., integrity protected and/or encrypted as per 3GPP NAS security requirements). The UE, upon receiving this protected deregistration message, did not respond further. According to the 3GPP 5G standard (TS 24.501), after the registration procedure is completed and if the UE receives a protected deregistration message from the AMF, it is expected to process the message and, unless otherwise specified (such as in the case of certain deregistration types), no further response is required from the UE. The key security consideration here is that the deregistration message from the AMF was protected, ensuring it was not spoofed or tampered with, and that the UE did not act on any unprotected or unauthenticated messages. Therefore, the UE's behavior aligns with the expected secure operation as per 3GPP standards, as it only responded to protected messages after security activation and did not respond to any potentially insecure or unexpected messages. Secure

121	121	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 1.719182014465332 UE to AMF SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, Authentication response 1.7194299697875977 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated NAS communication and proceeded to send an Authentication Response to the AMF before the 5G-AKA (Authentication and Key Agreement) procedure was completed. The AMF, under test control, responded with a Service Reject message using a plain (unencrypted) NAS message with 5GMM Cause 111 ("Protocol error, unspecified"). According to the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as encryption and integrity protection are only activated after successful authentication and key agreement. The UE, upon receiving the Service Reject message in plain text, did not respond further, which is appropriate since the session was terminated by the network and no security context had been established. Therefore, the UE's behavior—sending the Authentication Response in plain, accepting a plain Service Reject, and not responding further—is consistent with 3GPP security requirements for this stage of the protocol. There is no indication that the UE accepted or processed any unauthorized or unexpected messages, nor did it attempt to continue communication insecurely after the Service Reject. Thus, the UE acted securely according to the standard. Secure
122	122	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003769397735595703 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a Service Reject message, specifically indicating "UE identity cannot be derived by the network" (5GMM Cause 9). Importantly, this Service Reject was sent as a plain (unencrypted) NAS message, which is expected since the 5G-AKA authentication and key agreement procedure had not yet been completed—meaning no NAS security context was established. According to the 3GPP 5G standard (TS 24.501), initial NAS messages prior to authentication (such as registration requests and reject messages) are permitted to be sent in plain text, as encryption and integrity protection are only enabled after successful authentication and security mode command procedures. The UE, upon receiving the plain Service Reject, did not respond further, which is compliant with the standard: the UE should not attempt further NAS procedures until a new registration attempt is made, as its identity was not accepted by the network. Thus, the UE's behavior—sending its initial registration in plain text, then ceasing communication after a plain Service Reject—aligns with 3GPP security requirements and does not expose it to additional risk in this context. Secure

123	123	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.03993701934814453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04126906394958496 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.24338102340698242 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an identity response to the AMF, the AMF responded with a Security Mode Command message that was integrity protected and indicated the use of new security context, specifying cipher and integrity algorithms. However, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security keys for encryption and integrity protection had not been established. According to the 3GPP 5G standard, the Security Mode Command should only be sent after successful authentication (i.e., after 5G-AKA is completed), as only then are the required keys available for securing NAS messages. The UE, upon receiving a Security Mode Command before authentication was completed, rejected the command with a "Security mode rejected, unspecified" message. This behavior aligns with the 3GPP standard, as the UE should not accept security procedures or attempt to establish ciphering/integrity protection before the authentication process is finished and security contexts are derived. By rejecting the premature Security Mode Command, the UE prevented a potential security risk where messages could be protected with invalid or missing keys, thus maintaining the integrity of the security procedure. Therefore, the UE's action was secure and compliant with the 5G standard. Secure
124	124	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03973102569580078 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003596305847168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24200010299682617 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). After completing the initial NAS steps, the UE sent an identity response, and the AMF subsequently issued another identity request, specifically requesting the Subscription Concealed Identifier (SUCI). The UE then responded with another identity response. Importantly, the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established, and all messages exchanged—including the identity responses—were sent in plain (unencrypted) form. According to the 3GPP 5G standard, it is expected that the initial identity exchange (such as SUCI) can occur before the completion of 5G-AKA, and thus before NAS security is activated. The SUCI is specifically designed to protect the subscriber's permanent identifier (SUPI) by using public key encryption, so that even when sent in the clear, the SUPI is not exposed. Therefore, the UE's action of sending the SUCI in response to a plain identity request prior to NAS security activation is compliant with the 3GPP standard and does not expose sensitive information. Based on this, the UE's behavior in this interaction was secure. Secure

125	125	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00029206275939941406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the initial NAS messages exchanged before the completion of 5G-AKA (such as registration requests and authentication challenges/rejects) are permitted to be sent in plain text, as security context and encryption keys are not yet established. The UE, upon receiving an Authentication Reject message before authentication is completed, is expected to not respond further and to abort the registration process, as it cannot verify the authenticity of the network at this stage. In this test, the UE did not respond to the plain Authentication Reject message, which aligns with the 3GPP security recommendations to avoid further interaction when authentication has not been established and a reject is received. This behavior prevents potential exploitation by malicious actors attempting to spoof network messages prior to authentication. Therefore, the UE's action was in accordance with the 5G security standard and did not expose itself to additional risk in this scenario. Secure
126	126	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5059909820556641 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5062329769134521 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7099969387054443 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration process was finalized. Immediately following this, the AMF (under test control) sent a "Deregistration Request (UE terminated)" message to the UE, which was integrity protected and ciphered, as indicated by the security header (2). The UE responded appropriately with a "Deregistration Accept (UE terminated)" message, acknowledging the request. According to the 3GPP 5G standards, after 5G-AKA is completed, all subsequent NAS messages—including deregistration procedures—must be both integrity protected and ciphered to ensure confidentiality and authenticity. The packet capture confirms that the deregistration request from the AMF was indeed protected, and the UE responded as specified by the standard. The UE did not accept or process any unprotected or unexpected messages, and its actions were in line with the security requirements for NAS message handling post-authentication. Therefore, the UE's behavior in this interaction was secure and compliant with 3GPP specifications. 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 to the AMF, which is expected to occur in plain (unencrypted) NAS since the 5G-AKA authentication and key agreement had not yet been completed. The AMF, under test control, then sent a Deregistration Accept message in plain NAS to the UE. The UE did not respond further after receiving this message. According to the 3GPP 5G standard, NAS messages prior to the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as encryption and integrity protection are not yet available. The UE's behavior—sending the Identity Response in plain and not responding to the Deregistration Accept—aligns with expected protocol operation, as it did not attempt to establish a secure context before authentication was complete, nor did it process further after being deregistered. There is no indication that the UE inappropriately accepted or processed messages that should have been protected, nor did it continue communication after deregistration. Therefore, the UE's actions were in accordance with the 3GPP security requirements for this stage of the NAS procedure. Secure
128	128	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3031 RAND: 00000000000000000000000000000000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Mapped security context ngKSI_KSI: 1 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.03987288475036621 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04013490676879883 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24352788925170898 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an identity response to the AMF, the AMF replied with an authentication request message that was sent in plain (unencrypted) form, with both the RAND and AUTN fields set to all zeros—values that are clearly invalid for a legitimate authentication challenge. The UE, upon receiving this malformed authentication request, did not proceed with the authentication process but instead responded with a 5GMM status message indicating "Invalid mandatory information." This behavior shows that the UE correctly detected the invalidity of the authentication request and refused to process it further, as required by the 3GPP 5G security standards. According to 3GPP specifications, the UE must not accept or process authentication requests that are malformed, contain invalid parameters, or are sent in plain text before the security context is established. By refusing to proceed and reporting the error, the UE prevents potential security vulnerabilities such as replay or downgrade attacks that could arise from processing unauthenticated or tampered messages. Therefore, the UE's action aligns with the security requirements of the 5G standard and demonstrates secure behavior in this context. 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 successful completion of the 5G-AKA authentication procedure, the UE responded to the AMF with an authentication response. The AMF then sent a Security Mode Command to the UE, which was integrity protected using the new security context, with the ciphering algorithm set to 5G-EA0 (null, meaning no encryption) and the integrity algorithm set to 128-5G-IA2. Upon receiving this command, the UE rejected the security mode, responding with a Security Mode Reject message, citing an unspecified reason. According to the 3GPP 5G standard, after authentication, the network should select both integrity and ciphering algorithms to protect NAS signaling. The use of 5G-EA0 (null ciphering) means that subsequent NAS messages would not be encrypted, only integrity protected. Many 5G UEs are designed to reject security mode commands that select null ciphering (5G-EA0) in commercial deployments, as this could expose sensitive signaling information over the air and is generally considered insecure except for specific, controlled scenarios (e.g., emergency services or regulatory requirements). The UE's rejection of the security mode command when null ciphering was proposed is therefore a secure and standards-compliant action, as it prevents the establishment of an insecure signaling session. The UE's behavior demonstrates proper security posture by refusing to proceed with unencrypted NAS signaling, thus protecting user privacy and network integrity. Secure

130	130	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3131 RAND: 35353535353535353535353535353535 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.04801797866821289 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04822111129760742 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.25036191940307617 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an identity response, the AMF replied with an authentication request message that was transmitted in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. The UE, upon receiving this authentication request, responded with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should only accept authentication requests that conform to 5G-AKA and should reject any authentication procedures that do not meet the required security context or are not protected as specified. Since the authentication request was sent in plain text and before the establishment of a secure context, the UE correctly identified this as a non-5G compliant authentication attempt and refused to proceed, thereby protecting itself from a potential downgrade or interception attack. This behavior aligns with the security requirements of the 5G standard, demonstrating that the UE is enforcing proper security checks and not accepting insecure or non-standard authentication procedures. Secure
131	131	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 26 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00038909912109375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a registration reject message using 5GMM Cause 26 ("Non-5G authentication unacceptable"), and this message was sent in plain (unencrypted) form. The 5G-AKA authentication procedure had not yet been completed, which is a prerequisite for establishing NAS security (encryption and integrity protection of NAS messages). According to the 3GPP 5G standard (TS 24.501), before the completion of 5G-AKA and the establishment of NAS security, both the registration request from the UE and the registration reject from the AMF are expected to be sent in plain text. The UE, upon receiving the registration reject, did not respond further, which is compliant with the standard behavior when registration is rejected prior to authentication. Therefore, the actions taken by the UE—sending its initial registration request in plain text, accepting the plain-text registration reject, and not responding further—are fully in line with 3GPP security procedures for this phase of communication. The UE did not expose itself to any additional security risk beyond what is permitted by the standard at this stage. 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 the initial NAS procedures and sent an Identity Response message to the AMF in plain (unencrypted) NAS, as the 5G-AKA authentication and key agreement procedure had not yet been completed. The AMF, under test control, responded with a Service Reject message, also in plain NAS, with a 5GMM cause value of 99 ("Information element non-existent or not implemented"). Following this, the UE did not respond further. According to the 3GPP 5G standard, it is expected that all NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are sent in plain text, as encryption and integrity protection are only activated after successful authentication and key agreement. The UE's behavior—sending the Identity Response in plain text and ceasing communication after receiving a Service Reject—aligns with the standard and does not expose the UE to additional risk, since no sensitive user data is transmitted before security activation. Therefore, the UE's actions in this scenario are consistent with 3GPP security requirements and do not constitute a security vulnerability. 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 replied with an authentication request message that was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. The UE, upon receiving this unprotected authentication request, responded with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security standards, the authentication and key agreement procedure (5G-AKA) must be completed before any sensitive NAS messages are exchanged in a protected (encrypted and integrity-protected) manner. The UE is expected to reject or not process authentication requests that are not compliant with 5G security requirements, such as those sent in plain text when a native 5G security context is expected. By refusing to proceed with authentication in response to an unprotected request, the UE demonstrated adherence to the 3GPP security guidelines, thereby preventing potential security vulnerabilities such as replay or interception attacks. This behavior ensures that the UE does not expose itself to risks by accepting or responding to insecure authentication procedures. Therefore, the UE's action in this scenario was secure and in line with 5G security standards. Secure

134	134	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 3 UE provided: No response The packet capture during the test using wireshark is: 0.039869070053100586 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040055036544799805 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service reject (Illegal UE) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). The UE, after completing the initial NAS steps, sent an Identity Response message in plain (unencrypted) form to the AMF, as the 5G-AKA authentication procedure had not yet been completed. The AMF then responded with a Service Reject message, also in plain form, with a 5GMM Cause value of 3 (Illegal UE). The UE did not respond further after receiving this reject message. According to the 3GPP 5G standard, NAS messages prior to the completion of 5G-AKA (i.e., before security context establishment) are exchanged in plain text, as encryption and integrity protection are only enabled after successful authentication and key agreement. The UE's behavior—sending the Identity Response in plain text before 5G-AKA and ceasing communication upon receiving a Service Reject—aligns with the expected and secure operation defined by the standard. The UE did not attempt to continue communication or respond inappropriately after being rejected, which further supports its compliance with security requirements. Therefore, the UE's actions in this interaction were secure according to the 3GPP 5G standard. Secure
135	135	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00067901611328125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.2038860321044922 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF responded with a Security Mode Command, indicating the selection of null algorithms for both ciphering (5G-EA0) and integrity protection (5G-IA0), and marked the security header as "Integrity protected with new security context." However, the 5G-AKA authentication procedure, which is required to establish security keys for encryption and integrity protection, had not yet been completed. Upon receiving the Security Mode Command with null algorithms and without a completed authentication, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, the use of null algorithms (EA0/IA0) is only permitted under specific circumstances, and security procedures must not proceed without first completing authentication (5G-AKA) to derive the necessary keys. The UE's decision to reject the security mode command in this context aligns with the standard's security requirements, as accepting null algorithms without authentication would expose the communication to significant security risks. Therefore, the UE's actions demonstrate adherence to the 3GPP security framework and best practices for protecting user data and signaling. 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, the UE and AMF engaged in NAS communication where, after the UE sent an identity response, the AMF responded with a Security Mode Command. Notably, the Security Mode Command was sent as a protected message, specifying the use of the null ciphering algorithm (5G-EA0) and the integrity algorithm 128-5G-IA3, with the security header indicating integrity protection with a new security context. However, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that the necessary security context and keys for encryption and integrity protection had not been established. According to the 3GPP 5G standards, the Security Mode Command should only be sent after successful authentication (i.e., after 5G-AKA is completed), as the UE cannot securely derive or use the required keys beforehand. The UE, recognizing that the security context was not yet valid, responded with a Security Mode Reject message, indicating that it could not accept the security mode command under these circumstances. This behavior aligns with the security expectations of the 5G standard, as the UE refused to proceed with security procedures without proper authentication, thereby preventing potential security vulnerabilities such as accepting unauthenticated or improperly protected messages. Therefore, the UE's action was secure and compliant with 3GPP standards. Secure

137	137	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 2f4b62abf69d8352398c608fb3a89563 AUTN: 062d8ab6b7549000811f4ee8b8da8440 ngKSI_TSC: Native security context ngKSI_KSI: 6 UE provided: Authentication response The packet capture during the test using wireshark is: 1.9198977947235107 UE to AMF SACK (Ack=5, Arwnd=106496) , UplinkNASTransport, Authentication response 1.9201328754425049 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Authentication request 2.120612859725952 UE to AMF UplinkNASTransport, Authentication response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF are engaged in the NAS authentication procedure, specifically the 5G-AKA process. After the initial NAS steps, the UE sent an Authentication Response to the AMF. However, instead of proceeding to the Security Mode Command (which would establish NAS encryption and integrity protection), the AMF sent another Authentication Request to the UE, and this message was sent in plain (unencrypted) form. The UE then responded with another Authentication Response. According to the 3GPP 5G standard, NAS messages prior to the completion of authentication and security mode setup are permitted to be sent in plain text, as encryption and integrity protection are not yet established. However, the UE should only respond to valid authentication requests and should not continue to process repeated or unexpected authentication requests after it has already provided a valid Authentication Response, as this could be indicative of a replay or downgrade attack. In this scenario, the UE responded to a repeated Authentication Request after already completing its part of the authentication, which is not compliant with the expected behavior outlined in the standard. This could expose the UE to replay or reflection attacks, as it is not verifying the sequence or context of authentication requests. Therefore, the action taken by the UE is considered insecure according to the 3GPP 5G standard. Insecure

138	138	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5089499950408936 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5091559886932373 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7129359245300293 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context had been established and that subsequent NAS messages would be protected. Immediately after, the AMF sent a "Deregistration Request (UE terminated)" message to the UE, which was integrity protected and ciphered, as indicated by the security header (2). The UE then responded with a "Deregistration Accept (UE terminated)" message, completing the deregistration process. According to the 3GPP 5G standards, once the 5G-AKA procedure is completed, all subsequent NAS messages between the UE and the AMF must be both integrity protected and ciphered to ensure confidentiality and integrity. The packet capture confirms that the deregistration request from the AMF was protected, and the UE responded appropriately with a deregistration accept message. The UE did not process or respond to any unprotected NAS messages after security was established, and all its actions were in line with the expected 3GPP security requirements. Therefore, the UE's actions were secure and compliant with the 5G standard. 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 responded with an authentication request message, which was sent in plain (unencrypted) form, as the 5G-AKA authentication procedure had not yet been completed—this is expected, since encryption and integrity protection of NAS messages are only established after successful authentication and key agreement. The authentication request from the AMF included a RAND value and an AUTN value, but the AUTN was all zeros, which is not valid according to the 3GPP 5G security specifications (AUTN must be a valid authentication token generated by the network). Upon receiving this invalid authentication request, the UE responded with a 5GMM status message indicating "Invalid mandatory information," which is a standards-compliant way for the UE to signal that it received a malformed or non-compliant message. This behavior aligns with 3GPP requirements, as the UE must not proceed with authentication or provide sensitive information in response to an invalid or suspicious authentication challenge, especially before a secure context is established. The UE did not attempt to process the invalid AUTN or proceed with the authentication, thus protecting itself from potential security risks such as replay or man-in-the-middle attacks. Therefore, the UE's actions were secure and in accordance with the 3GPP 5G security standards. 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 responded with an authentication request message, which was sent in plain (unencrypted) form, as expected since the 5G-AKA authentication and key agreement procedure had not yet been completed. At this point, instead of proceeding with the authentication process (e.g., responding with an authentication response), the UE immediately sent a deregistration request (UE originating) to the AMF. According to the 3GPP 5G security standards, NAS messages exchanged before the completion of 5G-AKA are permitted to be sent in plain text, as no security context has been established yet. However, the UE's action to deregister immediately after receiving the authentication request, without attempting authentication, is unusual and could indicate a security concern or a defensive behavior (such as aborting the registration due to detecting an anomaly or unexpected condition). If the UE was programmed to abort registration upon receiving a plain authentication request (which is standard at this stage), this could be overly cautious or a misconfiguration, as the 5G standard expects the UE to respond to the authentication challenge before security is activated. Therefore, while the UE did not expose any sensitive information in plain text, its refusal to proceed with authentication does not align with the expected 3GPP procedure and could be considered insecure or non-compliant, as it prevents the establishment of a secure context and normal service. **Insecure**
141	141	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.17494893074035645 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.17513012886047363 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in the initial steps of NAS communication for 5G standalone, specifically during the authentication phase. The UE sent an authentication response to the AMF, after which the AMF replied with an authentication reject message. Notably, the authentication reject was sent in plain (unencrypted) form, which is expected since the 5G-AKA procedure had not yet been completed; encryption and integrity protection of NAS messages are only established after successful authentication and key agreement. The UE, upon receiving the authentication reject, did not respond further, which aligns with 3GPP standards—once authentication is rejected, the UE should not proceed with further NAS signaling for that session. The UE's actions—sending the authentication response in plain before security context establishment, and ceasing communication after receiving an authentication reject—are consistent with the expected behavior defined by the 3GPP 5G security architecture. Therefore, the UE acted securely within the context of the 5G standard. 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, which then replied with a new authentication request message. Notably, this subsequent authentication request from the AMF was sent in plain (unencrypted) form, even though the 5G-AKA procedure had not yet been completed, meaning that a secure context for encryption and integrity protection had not been established. Upon receiving this plain authentication request, the UE responded with an "Authentication failure (Non-5G authentication unacceptable)" message, indicating that it rejected the authentication attempt because it did not meet 5G security requirements. According to the 3GPP 5G security standards, after the initial authentication response, any further sensitive NAS messages, especially those related to authentication, should be protected (encrypted and integrity-protected) once a security context is established. The UE's refusal to accept a plain, unprotected authentication request aligns with the security principles of 5G, which are designed to prevent replay, interception, or manipulation of authentication messages. By rejecting the unprotected message, the UE demonstrated adherence to the 5G security standard and protected itself from potential security risks. Therefore, the UE's action 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, 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 was established and that subsequent NAS messages would be protected (integrity protected and ciphered). The AMF then sent a "Deregistration Request" message to the UE, which was correctly protected with integrity and ciphering, as indicated by the security header. However, the UE did not respond to this deregistration request. According to the 3GPP 5G standards (TS 24.501), upon receiving a protected deregistration request from the AMF, the UE is expected to process the message and send a deregistration accept message in response, also protected by NAS security. The lack of response from the UE suggests that it did not handle the deregistration request as specified by the standard. This behavior could indicate a security or protocol handling issue on the UE side, as it failed to complete the expected secure deregistration procedure. Therefore, based on the 3GPP standard, the UE's action in this scenario is not compliant and is considered insecure. Insecure

144	144	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5077369213104248 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5080108642578125 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.7157459259033203 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration process was finalized. Subsequently, the AMF sent a "Configuration Update Command" to the UE, which was transmitted as a protected NAS message—specifically, with both integrity protection and ciphering enabled, as indicated by the security header (value 2). The UE then responded with a "Configuration Update Complete" message, confirming receipt and processing of the command. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) must be activated only after successful authentication and security mode command exchange, which is implied here by the completion of 5G-AKA prior to the exchange of protected messages. The UE's actions—waiting for security activation before exchanging sensitive configuration information and responding appropriately with protected messages—align with the security requirements outlined by 3GPP for NAS communication. Therefore, the UE's behavior in this interaction was secure, as it adhered to the expected security procedures for protecting NAS messages after authentication and key establishment. Secure
145	145_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.15980100631713867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16017889976501465 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3686530590057373 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the negotiated security algorithms (ciphering: 5G-EA0 (null), integrity: 128-5G-IA2) and was ready to proceed with protected NAS communication. However, the AMF then sent another "security mode command" message to the UE, which is an unusual sequence since the security mode command is typically sent only once after authentication, and the UE should only respond with "security mode complete" once per security context establishment. The packet capture shows that the UE responded again with "security mode complete" after receiving this second security mode command. According to 3GPP standards, the UE should not accept a second security mode command with the same or a new security context unless there is a valid reason (such as a context loss or explicit re-authentication). Accepting and responding to repeated or unexpected security mode commands can expose the UE to replay or downgrade attacks, especially since the ciphering algorithm negotiated was 5G-EA0 (null), meaning no encryption was applied, although integrity protection was enabled. The UE's action of accepting and responding to a repeated security mode command without verifying its validity or context is not compliant with the expected secure behavior as outlined by 3GPP, as it could allow an attacker with AMF control to manipulate the security context or force the use of weaker security settings. Therefore, the UE's behavior in this test was insecure. Insecure

146	146	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.1601390838623047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037797927856445 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated NAS security algorithms and was ready to communicate securely. Immediately following this, the AMF sent a "deregistration accept" message, which was protected (i.e., integrity protected and/or ciphered) as expected after security activation. The UE, upon receiving this protected deregistration accept message, did not respond further. According to the 3GPP 5G standards (TS 24.501), after the security mode is complete and NAS security is activated, all subsequent NAS messages, including deregistration messages, must be protected. The UE's lack of response to a properly protected deregistration accept message is compliant with the standard, as the deregistration accept is a terminal message for the deregistration procedure and does not require an acknowledgment from the UE. Therefore, the UE's actions—activating security after 5G-AKA, sending security mode complete, and not responding to a protected deregistration accept—align with 3GPP security requirements and do not expose any security weaknesses in this context. 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, the UE and AMF completed the 5G-AKA authentication, establishing a secure context for NAS message protection. After the UE sent the "security mode complete" message, the AMF responded with a "configuration update command" that was integrity-protected and used the new security context, as indicated by the security header. The UE then replied with a 5GMM status message indicating "Message type not compatible with the protocol state." According to the 3GPP 5G NAS protocol (TS 24.501), after security mode completion, the UE should only accept certain messages in specific protocol states. If the AMF sends a message that is not allowed in the current state, the UE is expected to respond with a 5GMM status message indicating the incompatibility. This behavior is a security feature designed to prevent protocol confusion or exploitation by malicious network elements. Therefore, the UE's action—responding with a status message rather than processing an unexpected or out-of-sequence command—demonstrates adherence to the 5G standard and proper protocol state management. This response helps prevent potential attacks that could exploit state mismatches or force the UE into an invalid state. Based on this analysis, the UE's actions were secure and in line with 3GPP specifications. Secure

148	148	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.11970210075378418 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.11996603012084961 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (5G-AKA and security mode complete) 0.3268871307373047 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (integrity protection and ciphering) was now active. Subsequently, the AMF issued a deregistration request to the UE, which was sent as a protected message (with both integrity protection and ciphering enabled, as indicated by the security header value of 2). The UE responded with a deregistration accept message, completing the deregistration process. According to the 3GPP 5G standard, once NAS security is established (after 5G-AKA and security mode complete), all subsequent NAS messages exchanged between the UE and the AMF must be protected. The packet capture confirms that the deregistration request from the AMF was indeed protected, and the UE responded appropriately. There is no indication that the UE accepted or processed any unprotected NAS messages after security activation, nor did it send unprotected messages itself. Therefore, the UE's actions align with the security requirements of the 5G standard, ensuring that sensitive signaling was not exposed. Secure
149	149	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected (1) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.16007494926452637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037607192993164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.364534854888916 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the security algorithms and parameters proposed by the network. However, the AMF then sent a "security mode command" message to the UE, which is unusual because, according to the 3GPP 5G standard (TS 24.501), the "security mode command" should be sent by the AMF before the UE responds with "security mode complete." The correct sequence is: AMF sends "security mode command" (protected by the NAS security context established after 5G-AKA), and then the UE responds with "security mode complete." In this test, the UE sent a second "security mode complete" after receiving another "security mode command" from the AMF, which is not compliant with the standard sequence. This could indicate that the UE is not properly tracking the security context or is accepting repeated or out-of-order security mode commands, which could be exploited by an attacker to perform downgrade or replay attacks. Therefore, the UE's behavior in this scenario is not secure according to the 3GPP 5G standard, as it should not respond to a second "security mode command" after already completing the security mode procedure. 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) (AMF initiated) 0.3618440628051758 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message, indicating that NAS security procedures (integrity protection and ciphering) were established. Subsequently, the AMF sent a "deregistration request" message, which was protected with both integrity and ciphering, as indicated by the security header (2). The UE responded with a "deregistration accept" message, also under NAS security protection. According to the 3GPP 5G standard, once NAS security is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and ciphered to prevent interception or tampering. The UE's actions—responding only after security was established and sending its deregistration accept message under protection—demonstrate compliance with these requirements. There is no indication that the UE accepted or responded to any unprotected or insecure messages after security was activated. Therefore, based on the observed behavior and adherence to 3GPP security procedures, the UE acted securely in this interaction. Secure
151	151	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00026297569274902344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an InitialUEMessage containing a Registration Request to the AMF. In response, the AMF sent an Identity Request message, specifically requesting the UE's GUTI (Globally Unique Temporary Identifier). Importantly, this Identity Request was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed—meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G security standards, the UE should avoid sending any permanent or sensitive identifiers (such as SUPI or IMSI) in plain text before NAS security is activated, but it is generally considered acceptable to send temporary identifiers like the GUTI in plain text at this stage. However, if the UE does not have a valid GUTI or is unsure of the security context, it is also compliant for the UE to not respond or to wait for a secure channel before providing any identity. In this test, the UE did not respond to the plain-text Identity Request for GUTI, which demonstrates a cautious approach and avoids the risk of exposing any identifier—even a temporary one—over an unprotected channel. This behavior aligns with a conservative interpretation of 3GPP security guidelines, prioritizing the protection of the UE's identity information until a secure context is established. Therefore, the UE's action in this scenario can be considered secure. Secure

152	152	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007770061492919922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, before completing the 5G-AKA authentication and key agreement procedure (which is necessary to establish NAS security), responded with a DownlinkNASTransport message carrying a Configuration Update Command. This downlink message was marked as "Protected," but the security header was "Unknown," and crucially, the 5G-AKA procedure had not yet been completed. According to the 3GPP 5G standard (TS 24.501), NAS security (encryption and integrity protection) must not be applied to messages until after the successful completion of authentication and security mode command procedures. The UE, upon receiving a protected message before security context establishment, did not respond. This behavior aligns with the 3GPP standard, as the UE should ignore or discard NAS messages that are protected before security activation, to prevent potential security vulnerabilities such as replay or spoofing attacks. Therefore, the UE's action of not responding to the prematurely protected message was correct and secure according to the standard. 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, after the UE sent an initial registration request to the AMF, the AMF responded with a Security Mode Command message that was protected using the security header "Integrity protected with new security context (3)", ciphering algorithm 128-5G-EA3, and integrity algorithm 5G-IA0 (null). However, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for encryption and integrity protection had not been established between the UE and the network. Upon receiving the Security Mode Command, the UE responded with a 5GMM status message indicating "Invalid mandatory information". According to the 3GPP 5G standards (TS 24.501 and TS 33.501), the UE must not accept security-protected NAS messages (i.e., messages with integrity protection or ciphering) before the successful completion of the authentication procedure (5G-AKA), as the required keys and context are not yet available or valid. By rejecting the Security Mode Command with an error status, the UE correctly identified that the message was not valid in this context and did not proceed with insecure or unauthorized security procedures. This behavior aligns with the 3GPP security requirements and demonstrates that the UE did not accept potentially insecure communication. Secure

154	154	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0009160041809082031 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF, which is the expected first step in establishing a connection. The AMF, under test control, responded with a configuration update command that was integrity protected and ciphered, as indicated by the security header (2). However, the critical detail is that the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed at this point. According to the 3GPP 5G standard, security procedures—specifically, the establishment of NAS security context through 5G-AKA—must be completed before any NAS messages are sent with integrity protection and ciphering. Since the UE had not yet completed 5G-AKA, it did not possess the necessary keys to decrypt or verify the integrity of the protected configuration update command. The UE's lack of response to this message is therefore correct and secure behavior, as it prevents the processing of potentially spoofed or unauthorized messages before security has been established. This action aligns with 3GPP security requirements, which mandate that UEs must ignore NAS messages that are protected before security context is established. Thus, the UE's behavior in this scenario was secure. Secure
155	155	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00041294097900390625 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF, as indicated by the "InitialUEMessage, Registration request" in the packet capture. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed—which is required to establish security context and enable encryption and integrity protection—the AMF responded with a "Deregistration accept" message, which was marked as "Protected." According to the 3GPP 5G standards, specifically TS 33.501, NAS message protection (encryption and integrity) should only be applied after successful completion of the authentication and security setup (i.e., after 5G-AKA). Since the UE had not yet established a security context, it would not have the necessary keys to decrypt or verify the integrity of the protected message from the AMF. The UE's action of not responding to the protected "Deregistration accept" message is therefore correct and secure, as it avoids processing a message that it cannot verify or decrypt, in compliance with the 3GPP security requirements. This behavior prevents potential security vulnerabilities, such as accepting spoofed or malformed protected messages before security is established. Secure

156	156	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007860660552978516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.2037971019744873 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF responded with a Security Mode Command, which was sent as a protected message but specified the use of null algorithms for both ciphering (5G-EA0) and integrity protection (5G-IA0), and indicated a new security context. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that no valid security context or keys had been established between the UE and the network. Upon receiving the Security Mode Command with null algorithms and without a completed authentication, the UE responded with a Security Mode Reject, citing an unspecified reason. According to the 3GPP 5G standard, the UE must not accept a security context that uses null algorithms unless explicitly allowed by policy, and it should not proceed with security procedures before 5G-AKA is completed and keys are established. The UE's refusal to accept the insecure security mode command (with null algorithms and without authentication) demonstrates adherence to the security requirements of the standard, as it prevents the establishment of an unprotected or weakly protected communication channel. Therefore, the UE's action in rejecting the security mode command in this context was secure and compliant with 3GPP specifications. 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) (1 switch off) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that mutual authentication and the establishment of NAS security (integrity and ciphering keys) had not occurred. The AMF, under tester control, responded with a DownlinkNASTransport message containing a Deregistration Request, which was sent with a security header indicating integrity protection and ciphering (security header type 2). According to the 3GPP 5G standard, NAS messages that are integrity protected and ciphered must only be sent after successful completion of the 5G-AKA procedure, as the required security context and keys are not established prior to authentication. The UE, upon receiving a protected message before security context establishment, did not respond to the deregistration request. This behavior aligns with the 3GPP standard, which mandates that the UE should ignore or discard any NAS message that is protected before security activation. Therefore, the UE's action in not responding to the prematurely protected message was secure and compliant with the 5G security requirements. Secure

158	158	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03999805450439453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04024100303649902 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, and the AMF subsequently sent another Identity Request asking for the IMEISV, with the message transmitted in plain (unencrypted) form. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established between the UE and the AMF. According to 3GPP standards (TS 24.501), sensitive information such as the IMEISV should not be transmitted over unprotected NAS messages to prevent exposure of device identifiers to potential attackers. The UE, recognizing that the request for IMEISV was sent in plain text before the establishment of NAS security, chose not to respond. This behavior aligns with the security requirements outlined in the 3GPP standards, which recommend that the UE should not disclose sensitive identifiers like the IMEISV unless a secure NAS connection is in place. Therefore, the UE's action of withholding the IMEISV in the absence of NAS security demonstrates compliance with best security practices and the 3GPP standard. Secure
159	159	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 13 UE provided: No response The packet capture during the test using wireshark is: 0.03987693786621094 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04032492637634277 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Roaming not allowed in this tracking area) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and the AMF engaged in NAS communication where the UE sent an Identity Response message to the AMF, and the AMF subsequently sent a GMM Status message with a 5GMM cause value of 13 ("Roaming not allowed in this tracking area"). The packet capture shows that both messages were sent in plain (unencrypted) form, which is expected because the 5G-AKA authentication procedure had not yet been completed; encryption of NAS messages is only mandated after successful authentication and key agreement. Upon receiving the plain GMM Status message from the AMF, the UE did not respond. According to the 3GPP 5G standard (TS 24.501), before security activation, the UE is permitted to process certain plain NAS messages, including status messages, but is not required to respond to them, especially if the message indicates an error or unsupported operation. The UE's lack of response to the plain GMM Status message is therefore compliant with the standard and does not expose it to additional security risks, as it did not process or act upon potentially unauthenticated instructions. This behavior demonstrates that the UE did not perform any insecure actions during this exchange, as it adhered to the expected security procedures prior to the completion of 5G-AKA. Secure

160	160	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.038893938064575195 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039427995681762695 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF were engaged in NAS communication as part of the 5G standalone authentication and security procedures. The UE sent an Identity Response message to the AMF, after which the AMF sent a Configuration Update Command back to the UE. Notably, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet activated. The Configuration Update Command from the AMF was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), the UE should not process or respond to NAS messages that are not protected by security after the security context is expected to be established, or before the security mode command is completed. Since the 5G-AKA was not completed and the message was sent in plain, the UE's lack of response to the unprotected Configuration Update Command is consistent with the security requirements of the standard, as processing such messages could expose the UE to security risks such as spoofing or manipulation. Therefore, the UE's action in this scenario was secure and in line with 3GPP specifications. 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) completed the initial NAS steps and sent an Identity Response to the Access and Mobility Management Function (AMF). Immediately after, the AMF sent a Deregistration Accept message to the UE, which was marked as "Protected." However, the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed at this point in the exchange. According to the 3GPP 5G security standards, NAS message protection (integrity and encryption) is only possible after the successful completion of 5G-AKA, as this procedure establishes the necessary security context and keys for protecting subsequent NAS messages. Since the Deregistration Accept message from the AMF was sent as "Protected" before 5G-AKA was completed, the UE would not have the required security context to process or respond to this protected message. The UE's lack of response in this situation is therefore correct and aligns with the 3GPP standard, as it should not process or acknowledge protected messages without an established security context. This behavior prevents potential security vulnerabilities such as accepting or acting upon messages that could be spoofed or manipulated before mutual authentication and key agreement. Thus, the UE's action in this scenario was secure. Secure

162	162	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.03969311714172363 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003500938415527 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is a standard unprotected message sent prior to the completion of 5G-AKA authentication. The AMF, under test control, responded with a DownlinkNASTransport containing a Service Accept message, but crucially, this message was sent as "protected" (i.e., integrity protected and/or encrypted) even though the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G standard, NAS message protection (encryption/integrity) must only be applied after successful completion of 5G-AKA, when security context and keys are established. The UE, upon receiving a protected NAS message before the establishment of a security context, did not respond. This behavior aligns with the 3GPP standard, which requires the UE to ignore or discard protected NAS messages if security has not been activated. By not responding, the UE avoided processing a message that could not be securely validated, thereby preventing potential security vulnerabilities such as replay or downgrade attacks. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure
163	163	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.039769887924194336 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0399930477142334 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (UnsecAKA) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an Identity Response message to the AMF, which is a standard step prior to authentication. However, before the 5G-AKA authentication and key agreement procedure was completed, 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, even though the 5G-AKA procedure—which establishes the security context and keys for such protection—had not yet been completed. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) must only be applied after successful completion of 5G-AKA, as the necessary security context is not available beforehand. The UE, upon receiving a protected message before security context establishment, did not respond to the Deregistration Request. This behavior is compliant with the 3GPP standard, as the UE should discard or ignore protected messages if security context has not been established, thereby preventing potential security vulnerabilities or protocol confusion. Therefore, the UE's action in not responding to the prematurely protected message was secure and in line with 3GPP specifications. Secure

164	164	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.03993701934814453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04126906394958496 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.24338102340698242 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication where, after the UE sent an identity response, the AMF issued a Security Mode Command that was integrity protected and indicated the use of new security context, ciphering, and integrity algorithms. However, the critical point is that the 5G-AKA authentication procedure had not yet been completed, which means that the necessary security context for establishing keys and enabling protected NAS communication was not yet in place. According to 3GPP standards (TS 33.501 and TS 24.501), the Security Mode Command should only be accepted by the UE after successful completion of authentication (5G-AKA), as this ensures that both parties have derived the same security keys. Since the AMF sent a protected Security Mode Command before authentication was complete, the UE correctly rejected this command with a Security Mode Reject message, as accepting it could have led to insecure communication or key mismatches. This behavior aligns with the 3GPP security requirements, as the UE must not proceed with security activation until authentication is complete and keys are established. Therefore, the UE's action was secure and compliant with the 5G standard. Secure
166	166	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.07990884780883789 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response 0.0801239013671875 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication, where the UE sent an authentication response to the AMF, but the 5G-AKA authentication procedure had not yet been completed. Immediately after, the AMF sent a configuration update command to the UE, which was integrity protected but not encrypted, as indicated by the security header and the fact that 5G-AKA had not been completed. The UE did not respond to this configuration update command. According to the 3GPP 5G standards, NAS security (integrity protection and encryption) must only be applied after successful completion of the 5G-AKA procedure, which establishes the necessary security context. Since the 5G-AKA was not completed, the UE correctly did not respond to a protected message, as it had not yet established the security context required to process such messages. This behavior prevents potential security vulnerabilities that could arise from processing protected messages without proper key material. Therefore, the UE's action in not responding to the configuration update command before the completion of 5G-AKA aligns with 3GPP security requirements and is considered secure. Secure

167	167	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.07818889617919922 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response 0.07842707633972168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the IMEISV, but sent this request as a plain (unencrypted) NAS message before the completion of the 5G-AKA procedure. The UE did not respond to this identity request. According to the 3GPP 5G security standards (TS 33.501), sensitive information such as the IMEISV should not be transmitted in plain text before the security context is established, which only occurs after the successful completion of the 5G-AKA authentication and key agreement procedure. Since the AMF sent the identity request before security activation, it was not protected, and the UE's refusal to respond prevented the exposure of its IMEISV in an unprotected message. This behavior aligns with the security requirements set by 3GPP, as the UE must not send sensitive identifiers in clear text prior to the establishment of NAS security. Therefore, the UE's action in this scenario was secure. Secure
168	168	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.24675607681274414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.24697303771972656 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Service accept 0.4485650062561035 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE sent an authentication response to the AMF, after which the AMF replied with a service accept message that was protected (i.e., integrity protected and/or encrypted). However, the 5G-AKA (Authentication and Key Agreement) procedure, which is responsible for establishing security keys and enabling NAS message protection, was not completed at this point. According to the 3GPP 5G standard, NAS message protection (encryption and integrity) should only be activated after successful completion of 5G-AKA, ensuring that both the UE and the network have derived the necessary security keys. In this case, the UE received a protected service accept message from the AMF before 5G-AKA was completed, and then proceeded to send a deregistration request. This is problematic because the UE should not accept or process protected NAS messages (or send further NAS messages) before security context establishment via 5G-AKA. By acting on a protected message before security activation, the UE is violating the expected security procedures, potentially exposing itself to security risks such as replay or spoofing attacks. Therefore, the UE's behavior in this scenario is not compliant with the 3GPP 5G security standards and is considered insecure. Insecure

169	169	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 26 UE provided: No response The packet capture during the test using wireshark is: 0.1594829559326172 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.15969610214233398 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Authentication Response to the AMF, indicating it was attempting to complete the 5G-AKA authentication procedure. However, before the authentication was completed, the AMF responded with a GMM Status message containing a 5GMM cause value of 26 ("Non-5G authentication unacceptable"), and this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as encryption and integrity protection are only activated after successful authentication and key agreement. The UE, upon receiving the GMM Status message indicating an unacceptable authentication, did not respond further, which aligns with expected behavior since the authentication procedure was not successfully completed and the network indicated that further communication was not acceptable. The UE did not proceed with any further NAS procedures or send sensitive information in the clear. Therefore, based on the 3GPP standard, the UE's actions were secure, as it followed the correct protocol sequence and did not expose itself to unnecessary risk by transmitting sensitive data before security activation. Secure
170	170	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.11972379684448242 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999678611755371 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS steps and sent an authentication response to the AMF, indicating that the 5G-AKA authentication procedure was still ongoing and not yet completed. Immediately after receiving the authentication response, the AMF sent a deregistration request to the UE, which was integrity protected and ciphered (security header type 2). According to 3GPP 5G standards, NAS message protection (integrity and ciphering) should only be applied after successful completion of the 5G-AKA procedure, as this is when the necessary security context and keys are established between the UE and the network. Since the 5G-AKA was not completed, the UE had not yet derived the required keys to process protected NAS messages. The UE, therefore, did not respond to the protected deregistration request, which is the correct and secure behavior as per the standard; responding to such a message without a valid security context could expose the UE to security vulnerabilities such as replay or spoofing attacks. Thus, the UE's lack of response demonstrates adherence to the 3GPP security requirements and proper handling of protocol procedures. Secure

171	171	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15981698036193848 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16000986099243164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent messages. However, the AMF then sent an "identity request" message for the IMEISV in plain (unencrypted) NAS, rather than a protected message. According to the 3GPP 5G standard (TS 24.501), once NAS security is established (after security mode complete), all subsequent NAS messages, including identity requests, must be integrity protected and, where applicable, encrypted. The UE, upon receiving an unprotected identity request after security activation, is expected to ignore or silently discard the message to prevent potential security breaches such as IMEI catching or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected identity request, which aligns with the security requirements of the 5G standard, as responding would have exposed sensitive information in an unprotected manner. Therefore, the UE's action was 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 successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (integrity and encryption) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE requesting the GUTI, but crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after security mode complete), the UE is required to only accept and respond to NAS messages that are integrity protected and, where applicable, encrypted. If the UE receives a plain (unencrypted) NAS message after security activation, it should ignore it and not respond, 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 plain identity request, which is the correct and secure behavior as per the 3GPP standard, as it prevents potential security vulnerabilities such as identity disclosure or replay attacks. Secure

173	173	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.15993309020996094 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16013097763061523 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) 0.3612639904022217 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was successfully completed, which should have established security keys for NAS message encryption and integrity protection. After this, the UE sent a "Security mode complete" message, indicating it had accepted the security context and was ready for secure NAS communication. However, the AMF then sent a "Service reject" message with 5GMM Cause 111 (protocol error, unspecified) in plain (unencrypted) format. According to the 3GPP 5G standard (TS 24.501), once the security context is established and the security mode is complete, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) "Service reject" message after security activation, responded by sending a "Deregistration request (UE originating)" message. The correct and secure behavior, as per the standard, is for the UE to ignore any unprotected NAS messages received after security activation, except for a few specific cases (such as "Security mode command" or "Deregister accept" under certain conditions), which do not include "Service reject." By responding to an unprotected "Service reject" message, the UE has violated the 3GPP security requirements, as it should have discarded the message and not acted upon it. This behavior could potentially be exploited by an attacker to disrupt service or trigger deregistration. Therefore, the actions taken by the UE in this scenario are not secure according to the 5G standard. Insecure
174	174	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: c2ada16de5afa04c9abbf0b2aba327aa AUTN: 3030303030303000ee55922b5d550000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.15995287895202637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16016292572021484 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after completing the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated NAS security algorithms and was ready to communicate securely. However, the AMF subsequently sent an "authentication request" message to the UE in plain (unencrypted) format, even though the security context should have been established at this point. According to the 3GPP 5G standard (TS 24.501), once the security mode command is completed and acknowledged by the UE, all subsequent NAS messages between the UE and the AMF must be integrity protected and, if required, ciphered. The UE, upon receiving a plain (unencrypted) authentication request after the security mode complete, did not respond. This behavior aligns with the 3GPP security requirements, as the UE must reject or ignore any NAS messages that are not properly protected after security activation. By refusing to respond to an improperly protected message, the UE demonstrated secure behavior according to the 5G standard. Secure

175	175	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.15975189208984375 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15996503829956055 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated NAS security algorithms and was ready to begin protected NAS communication. However, the subsequent "service accept" message sent by the AMF to the UE was transmitted in plain (unencrypted) text, rather than being protected by the agreed-upon NAS security context. According to the 3GPP 5G standard (TS 24.501), once the security mode command is completed and acknowledged by the UE, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, if required, ciphered. The UE, upon receiving an unprotected (plain) "service accept" message after security mode completion, is expected to discard the message and not respond, as accepting or processing unprotected NAS messages at this stage would expose the UE to security risks such as spoofing or replay attacks. In this test, the UE correctly provided no response to the unprotected "service accept" message, demonstrating compliance with the 5G security requirements and protecting itself from potential attacks. Therefore, the action taken by the UE was secure according to the 3GPP standard. Secure
176	176	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.47094106674194336 UE to AMF UplinkNASTransport, Registration complete 0.47116804122924805 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF. Subsequently, the AMF sent an "Identity Request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier). Notably, this identity request was sent as a plain (unencrypted) NAS message, despite the fact that 5G-AKA had already been completed and NAS security should have been activated. The UE, upon receiving this unprotected identity request, did not respond. According to the 3GPP 5G standard (TS 24.501), once NAS security is established after 5G-AKA, the UE is required to ignore any subsequent NAS messages that are not integrity protected and ciphered, except for a few specific message types (such as Service Request under certain conditions). Since the identity request was sent in plain text after security activation, the UE's refusal to respond aligns with the security requirements of the standard, preventing potential exposure of sensitive identifiers like the SUCI over an unprotected channel. Therefore, the UE's action was secure and compliant with the 5G security specifications. Secure

177	177	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3031 RAND: 1230c172c0fe20b56039f8264c2856d4 AUTN: 2d236d5db431900054adfe579b1ec661 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.4670701026916504 UE to AMF UplinkNASTransport, Registration complete 0.46730613708496094 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the 5G-AKA authentication procedure and then sent a "Registration Complete" message to the AMF. Following this, the AMF sent an "Authentication Request" message to the UE, but crucially, this message was sent in plain (unencrypted) form, even though the 5G-AKA procedure had already been completed and a native security context was established. According to the 3GPP 5G security standards (TS 33.501), after successful completion of 5G-AKA and establishment of a security context, 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) NAS message after security context establishment, is expected to reject the message and not respond, as processing such messages could expose it to security risks such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the plain "Authentication Request" message, which is the correct and secure behavior as per the 3GPP standard. This indicates that the UE properly enforced the security requirements by refusing to process or respond to unprotected messages after the security context was in place. Secure
178	178	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 6.593172073364258 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.593342065811157 AMF to UE SACK (Ack=24, Arwnd=106401) , DownlinkNASTransport, Identity request 6.797163009643555 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context should have been established and all subsequent NAS messages should be protected (integrity protected and ciphered) according to 3GPP standards (TS 33.501). However, the AMF, under test control, sent an "Identity Request" message in plain (unencrypted and unprotected) form, requesting the SUCI (Subscription Concealed Identifier) from the UE. Upon receiving this unprotected identity request after security activation, the UE did not respond with the requested identity; instead, it initiated a "Deregistration Request (UE originating)" message, effectively terminating its registration. According to 3GPP specifications, after NAS security is activated, the UE must not accept or respond to unprotected NAS messages except for a limited set of procedures (such as service reject or deregistration). The UE's action to deregister rather than respond to an unprotected identity request demonstrates correct and secure behavior, as it avoids exposing sensitive information in the clear and adheres to the security requirements of the 5G standard. Therefore, the UE's response in this scenario was secure. Secure

179	179	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.265115976333618 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2653589248657227 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.469132900238037 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA procedure, the UE sent a "Registration Complete" message to the AMF, indicating that security context establishment and mutual authentication had been achieved. Subsequently, the AMF sent a "Configuration Update Command" to the UE, but this message was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. Upon receiving this plain message, the UE responded by sending a "Deregistration Request (UE originating)" to the AMF. According to the 3GPP 5G security standards (TS 33.501), after the 5G-AKA procedure is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered. If the UE receives a plain NAS message after security context establishment, it is required to treat this as a protocol error and should not process the message further; instead, it may deregister or drop the connection to protect itself from potential security threats such as replay or man-in-the-middle attacks. In this test, the UE correctly identified the receipt of a plain NAS message after security activation and responded by deregistering, which is the expected secure behavior as per 3GPP standards. Therefore, the UE's action 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 5G-AKA authentication (which establishes security context for NAS message encryption and integrity protection), the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent a Configuration Update Command to the UE, but this message was sent as a plain (unencrypted and unprotected) NAS message, as indicated by the security header value of 0. Upon receiving this plain message, the UE responded with a Deregistration Request (UE originating), effectively terminating its registration with the network. According to the 3GPP 5G standard, once 5G-AKA is completed and a security context is established, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, encrypted. The UE is required to reject or ignore any downlink NAS messages that are not protected after security activation. In this case, the UE correctly identified that the Configuration Update Command was sent in plain text after security activation and responded by deregistering itself, which is a secure and standards-compliant behavior designed to prevent potential security breaches or replay attacks. Therefore, the UE's action demonstrates adherence to 3GPP security requirements and proper handling of insecure network behavior. Secure

181	181	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3100 RAND: 35353535353535353535353535353535 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 5 UE provided: No response The packet capture during the test using wireshark is: 2.4268798828125 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4271068572998047 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.42726993560791 AMF to UE DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Authentication Request message to the UE, but this message was sent in plain (unencrypted) text, and the UE did not respond to it. According to the 3GPP 5G security standards, after successful completion of 5G-AKA, a security context should be established and all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and encrypted. The UE is expected to reject or ignore any NAS messages received in plain text after security activation, as accepting or responding to such messages could expose the UE to security risks such as replay or man-in-the-middle attacks. In this case, the UE's action of not responding to the plain-text Authentication Request after 5G-AKA completion aligns with the security requirements of the 3GPP standard, as it prevents potential exploitation of unprotected messages. Therefore, the UE's behavior in this scenario was secure. Secure

182	182	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.5082509517669678 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 0.5084729194641113 AMF to UE SACK (Ack=7, Arwnd=106334) , DownlinkNASTransport, Configuration update command 0.5085830688476562 AMF to UE DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which should indicate that both sides have established security context and that subsequent NAS messages are expected to be integrity protected and ciphered as per 3GPP 5G security requirements (TS 33.501). However, the AMF responded with a Service Reject message that was sent in plain (unencrypted and non-integrity protected) format, with a 5GMM Cause value of 111 (Protocol error, unspecified). The UE, upon receiving this plain Service Reject message after security context establishment, did not respond further. According to 3GPP standards, after 5G-AKA completion, the UE must reject any downlink NAS messages that are not integrity protected and ciphered, as accepting plain messages at this stage would expose the UE to security vulnerabilities such as spoofing or replay attacks. The UE's lack of response to the unprotected Service Reject message demonstrates correct and secure behavior, as it did not process or act upon a message that violated the expected security protections. Therefore, the UE's actions were in line with 3GPP security requirements and protected against potential attacks. Secure

183	183	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 35353535353535353535353535353535 AUTN: 3030303030303000eeb598a00f560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5556139945983887 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.555833101272583 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5559549331665039 AMF to UE DownlinkNASTransport, Authentication request 0.7596380710601807 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending an Authentication Request message to the UE in plain (unencrypted) form. Notably, the 5G-AKA procedure, which is responsible for establishing mutual authentication and deriving security keys for NAS message protection, was already completed before this exchange. According to the 3GPP 5G security standards (TS 33.501), after successful 5G-AKA, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted to prevent interception or tampering. However, in this test, the AMF sent an Authentication Request in plain text after 5G-AKA completion, which is a protocol violation. The UE appropriately detected this unexpected and insecure message, responded by sending a Deregistration Request (UE originating), effectively terminating its connection to the network. This action by the UE aligns with the 3GPP security requirements, as the UE is expected to reject or deregister from the network if it detects that the security context is not being properly applied after authentication. The UE's decision to deregister rather than proceed with insecure communication demonstrates adherence to the standard and protects against potential security threats such as replay or man-in-the-middle attacks. Therefore, the UE's action was secure and compliant with 5G security requirements. Secure

184	184	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 4.666133165359497 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 4.66637396812439 AMF to UE SACK (Ack=10, Arwnd=106401) , DownlinkNASTransport, Configuration update command 4.666524171829224 AMF to UE DownlinkNASTransport, Identity request 4.8701331615448 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA (authentication 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, specifically requesting the IMEI, and this message was sent in plain (unencrypted) form. Instead of responding with the requested IMEI, the UE replied with a Deregistration Request (UE originating). According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages, especially those involving sensitive information such as device identity (IMEI), must be protected using NAS security (i.e., encrypted and integrity protected). The UE's decision to not respond to a plain (unencrypted) Identity Request for IMEI, and instead initiate deregistration, aligns with the security requirements, as it avoids exposing its IMEI over an unprotected channel. This behavior demonstrates that the UE is adhering to the 3GPP security guidelines by refusing to transmit sensitive information unless the NAS security context is active and the channel is secure. Therefore, the UE's actions in this scenario are considered secure. Secure
185	185	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 62 UE provided: No response The packet capture during the test using wireshark is: 2.4262688159942627 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4268429279327393 AMF to UE SACK (Ack=13, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.427194833755493 AMF to UE DownlinkNASTransport, Registration reject (No network slices available) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, indicating that a security context had been established and subsequent NAS messages should be protected (i.e., integrity protected and ciphered) as per 3GPP TS 24.501. However, the AMF responded with a Registration Reject message that was sent in plain (unencrypted and non-integrity protected) form, with 5GMM Cause 62 ("No network slices available"). According to 3GPP standards, once 5G-AKA is complete and a security context is in place, the UE must only accept NAS messages that are integrity protected (and, if applicable, ciphered). The UE, upon receiving a plain Registration Reject after security activation, correctly did not respond to this message, as accepting or acting on a plain message in this context would be a security vulnerability (e.g., allowing a malicious actor to spoof a Registration Reject and deny service to the UE). Therefore, the UE's action—providing no response to the unprotected Registration Reject—demonstrates compliance with 3GPP security requirements and is considered secure behavior. Secure

186	186	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3200 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 5.633437156677246 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 5.634006023406982 AMF to UE SACK (Ack=11, Arwnd=106496) , DownlinkNASTransport, Security mode command 5.634031057357788 UE to AMF SACK (Ack=8, Arwnd=106454) , UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message (PDU session establishment request) to the AMF. The AMF then responded with a Security Mode Command, which 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, the Security Mode Command is always sent in plain NAS, as it is the message that initiates the activation of NAS security (ciphering and integrity protection) between the UE and the AMF. Upon receiving the Security Mode Command, the expected behavior from a standards-compliant UE is to process the command, select the proposed ciphering and integrity algorithms, and respond with a Security Mode Complete message, which should be the first message protected with the negotiated security algorithms. However, in this test, instead of responding with Security Mode Complete, the UE immediately sent a Deregistration Request (UE originating), effectively aborting the registration and security setup process. This action is not compliant with the 3GPP standard, as the UE is expected to either accept the security mode or reject it with a Security Mode Reject message, not silently deregister. This behavior could indicate a security issue or a non-standard implementation in the UE, as it does not properly handle the security procedure as specified by 3GPP. Therefore, the UE's action in this scenario is considered insecure. Insecure
187	187	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 2.197134017944336 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 2.197467088699341 AMF to UE SACK (Ack=11, Arwnd=106334) , DownlinkNASTransport, Configuration update command 2.1975760459899902 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Identity Request message to the UE, specifically requesting the IMEISV (International Mobile Equipment Identity and Software Version). Notably, this Identity Request was sent in plain (unencrypted) NAS, despite the fact that 5G-AKA had already been completed and security context should have been established. According to 3GPP 5G security standards (TS 33.501 and TS 24.501), once the security context is active (i.e., after 5G-AKA), all subsequent NAS messages, including identity requests and responses, must be protected by NAS security (integrity protected and, where applicable, ciphered). The UE, upon receiving a plain (unencrypted) Identity Request after security activation, did not respond to the request. This behavior aligns with 3GPP security requirements, as the UE is expected to ignore or reject messages that are not properly protected after security activation, to prevent potential security breaches such as identity theft or tracking. Therefore, the UE's refusal to respond to an unprotected identity request after 5G-AKA demonstrates correct and secure behavior as per the 5G standard. Secure

188	188	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.8423888683319092 gNB to AMF UEContextReleaseComplete, InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.8428249359130859 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE successfully completed the 5G-AKA authentication procedure, which should have established security contexts for subsequent NAS message encryption and integrity protection. After authentication, the UE sent a Service Request to the AMF, which is a typical step for requesting network resources. However, the AMF responded with a Deregistration Accept message that was sent in plain (unencrypted) form. According to the 3GPP 5G security standard (TS 33.501), after successful 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be protected with encryption and integrity algorithms negotiated during authentication. The UE, upon receiving an unprotected (plain) NAS message after security context establishment, should not accept or process such a message and should instead ignore it or trigger a security error. In this test, the UE did not respond to the plain Deregistration Accept message, which indicates that it correctly rejected or ignored the insecure message as per 3GPP requirements. This behavior demonstrates that the UE is compliant with the 5G security standard, as it did not accept or act upon an unprotected NAS message after security activation. Secure
189	189	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 8.602246046066284 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.602970123291016 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a standard step to initiate further NAS signaling. The AMF then responded with a Security Mode Command, which is intended to establish NAS security by activating ciphering and integrity protection using the negotiated algorithms (5G-EA6 for ciphering and 128-5G-IA2 for integrity). However, the Security Mode Command message sent by the AMF was transmitted as a plain (unencrypted and non-integrity protected) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard, after 5G-AKA is completed, the Security Mode Command is the first message that can still be sent in plain, but all subsequent NAS messages from the UE must be protected using the negotiated security algorithms. In this test, the UE did not respond to the plain Security Mode Command, which suggests that the UE refused to proceed with NAS signaling until security was properly established. This behavior aligns with the security requirements of the 5G standard, as the UE should not send further sensitive information in plain after security context establishment. Therefore, the UE's action of not responding to an unprotected Security Mode Command was secure and compliant with 3GPP specifications. Secure

190	190	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1010 RAND: 7479eaccb74fb3be01aa8b2b6ff1abcb AUTN: dd84e27507488000bb521f82528f6f6e ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: No response The packet capture during the test using wireshark is: 16.614274978637695 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 16.614504098892212 AMF to UE SACK (Ack=22, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE 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) text rather than being protected by NAS security. The UE, upon receiving this unprotected Authentication Request, did not respond. According to the 3GPP 5G security standards, after the successful completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. The UE is expected to reject or ignore any NAS messages that are not properly protected after a security context has been established. By not responding to the unprotected Authentication Request, the UE adhered to the security requirements and did not risk exposing itself to potential replay or man-in-the-middle attacks. Therefore, the UE's action was in line with the 3GPP standard and demonstrated secure behavior. Secure

191	191_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1010 RAND: 765bcfb5ee4bd70eb854f2deac92aea9 AUTN: 7f72e2496ad28000fd0cf5cd8a2492b7 ngKSI_TSC: Native security context ngKSI_KSI: 4 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 8.671967029571533 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.672221899032593 AMF to UE SACK (Ack=14, Arwnd=106496) , DownlinkNASTransport, Authentication request 8.874675035476685 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. The AMF, under test control, responded with a new authentication request message sent in plain (unencrypted) form, despite the fact that a native security context (ngKSI) had already been established and was in use. Upon receiving this unexpected authentication request, the UE replied with an "Authentication failure (ngKSI already in use)" message, indicating that it recognized the reuse of the ngKSI and refused to proceed with redundant authentication. According to the 3GPP 5G security standards, after the 5G-AKA procedure is completed and a security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. The UE is also expected to reject any attempts to reuse or replay authentication requests with an already active security context, as this could be a security risk (e.g., replay or downgrade attack). By refusing to process the new authentication request and signaling the error, the UE demonstrated correct and secure behavior as per the 3GPP standard, ensuring that the integrity of the security context was maintained and that no sensitive information was exposed in plain text. Secure
192	192	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 35.06067895889282 UE to AMF SACK (Ack=27, Arwnd=106496) , UplinkNASTransport, Service request 35.06101393699646 AMF to UE SACK (Ack=36, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the 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, but crucially, this message was sent in plain (unencrypted) form, despite the fact that the security context should have been established following the completion of 5G-AKA. According to the 3GPP 5G security standards, once the security context is established, all subsequent NAS messages—including identity requests—must be integrity protected and, where possible, encrypted to prevent interception or manipulation by unauthorized parties. The UE, upon receiving an unprotected (plain) identity request after security activation, did not respond. This behavior aligns with 3GPP security requirements, which specify that the UE must not respond to NAS messages that are not properly protected after security has been activated, as responding could expose sensitive information (such as the TMSI) to potential attackers. Therefore, the UE's refusal to respond to the unprotected identity request demonstrates adherence to the 5G security standard and is considered a secure action. Secure

193	193	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 9.49011492729187 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.490720987319946 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a standard step for establishing a secure NAS signaling connection. The AMF responded with a Configuration Update Command, sent as a protected (i.e., integrity protected and/or ciphered) NAS message. However, the security header of the downlink message was marked as "Unknown," and the UE did not respond to this message. According to the 3GPP 5G standards, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and AMF must be integrity protected and, where applicable, ciphered. If the UE receives a NAS message with an unknown or invalid security header, or if the message is not properly protected, the UE is expected to discard the message and not respond, as a security measure to prevent potential attacks or protocol violations. In this scenario, the UE's lack of response to a message with an unknown security header aligns with the security requirements of the 5G standard, as it prevents the processing of potentially unprotected or malicious messages. Therefore, the UE's action in this test was secure. Secure
194	194	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 18.81248188018799 UE to AMF UplinkNASTransport, Service request 18.8126699924469 AMF to UE SACK (Ack=18, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is the expected behavior as the UE attempts to establish or resume a session. In response, the AMF sent an Authentication Reject message in plain (unencrypted) NAS, and the UE did not respond to this message. According to the 3GPP 5G security standard (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. A plain (unencrypted) Authentication Reject message after authentication completion is not compliant with the standard, and the UE is required to ignore such messages to prevent downgrade or spoofing attacks. The UE's lack of response to the plain Authentication Reject message demonstrates correct and secure behavior, as it did not process or act upon a message that violated security requirements. This adherence to the standard protects the UE from potential security threats that could arise from accepting unauthenticated or unprotected messages after authentication. Secure

195	195_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 9.680989980697632 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.681249141693115 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Identity request 9.884641170501709 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF issued an Identity Request message, specifically requesting the SUCI (Subscription Concealed Identifier), and this message was sent in plain (unencrypted) form. The UE then responded with an Identity Response message. According to the 3GPP 5G security standard (TS 33.501), once 5G-AKA is completed, NAS signaling messages exchanged between the UE and the AMF should be integrity protected and, where confidentiality is required, encrypted. Sensitive information such as the SUCI is designed to protect the subscriber's permanent identity (SUPI) even if sent in the clear, but after authentication, the expectation is that subsequent NAS messages, including identity procedures, should be protected. In this case, the UE accepted and responded to a plain (unencrypted) Identity Request after authentication was complete, which is not compliant with the 5G security requirements. The UE should have rejected or ignored unprotected NAS messages after security context establishment. Therefore, the UE's action was insecure, as it accepted and responded to an unprotected identity request after 5G-AKA completion, exposing itself to potential security risks such as replay or impersonation attacks. 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 successfully completing the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is the expected behavior for initiating further communication. The AMF then responded with a Configuration Update Command, sent as a protected (secured) NAS message. However, the UE did not respond to this protected downlink message from the AMF. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where required, ciphered. The Configuration Update Command is a standard NAS message that should be accepted and processed by the UE if it is properly protected. The fact that the UE did not respond could indicate that it either did not recognize the security header or was unable to process the protected message, which may suggest a failure to comply with the expected security procedures. However, from a security perspective, if the UE did not recognize the security context or found the message's security header to be unknown or invalid, refusing to respond is actually the correct and secure behavior to prevent potential security breaches or replay attacks. Therefore, the UE's action of not responding to a message with an unknown security header aligns with secure practices as outlined by 3GPP, as it avoids processing potentially malicious or malformed messages. Secure

197	197	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005860328674316406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated the NAS communication by sending an initial registration request to the AMF, which is the expected behavior when a UE attempts to connect to the 5G network. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed, the AMF responded with a deregistration request message that was integrity protected and ciphered, as indicated by the security header. According to the 3GPP 5G standard, security procedures such as integrity protection and ciphering of NAS messages should only be applied after the successful completion of the 5G-AKA, when both the UE and the AMF have established shared security keys. Since the 5G-AKA was not completed, the UE would not have the necessary keys to decrypt or verify the integrity of the protected message. The UE did not respond to this protected deregistration request, which aligns with the standard's expectation that the UE should ignore or discard NAS messages that are protected before security context is established. This behavior prevents potential security vulnerabilities, such as replay or spoofing attacks, that could arise if the UE processed protected messages without proper key agreement. Therefore, the UE's action of not responding to the prematurely protected deregistration request was secure and compliant with the 3GPP standard. Secure
198	198	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15979790687561035 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16023778915405273 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE requesting the GUTI, but this message was sent in plain (unencrypted) NAS, as observed in the packet capture. According to the 3GPP 5G standards (TS 24.501), once NAS security is established (i.e., after the security mode complete), all subsequent NAS messages between the UE and the AMF must be integrity protected and, if confidentiality is enabled, encrypted. The UE, upon receiving a plain (unencrypted) identity request after security activation, did not respond. This behavior aligns with the 3GPP standard, which states that the UE must ignore any NAS messages not protected according to the agreed security context after the security mode is complete. By refusing to respond to an unprotected message, the UE prevented a potential security vulnerability (such as a downgrade or replay attack), thereby maintaining the confidentiality and integrity of its identity. Therefore, the UE's action was secure and compliant with the 5G security requirements. Secure

199	199	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.1600339412689209 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602790355682373 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a Security Mode Complete message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an Identity Request message to the UE, requesting the IMEISV, but crucially, this message was sent in plain (unencrypted) form rather than being protected by the established NAS security context. According to 3GPP standards (TS 24.501), once NAS security is activated (i.e., after Security Mode Complete), the UE must only accept and respond to NAS messages that are integrity protected and, where required, encrypted. If the AMF sends a plain (unencrypted) NAS message after security activation, the UE is expected to ignore it and not respond, 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 plain Identity Request, which aligns with the security requirements specified by 3GPP. Therefore, the UE's action was secure, as it correctly refused to process or respond to an insecure request after NAS security was established. Secure
200	200	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.1511218547821045 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15138006210327148 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an Identity Request message to the UE in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier). The UE did not respond to this request. According to the 3GPP 5G standards (TS 24.501), once NAS security is activated (after Security Mode Complete), all subsequent NAS messages between the UE and the AMF must be protected (i.e., encrypted and integrity protected). The SUCI is a privacy-sensitive identifier, and the standard explicitly prohibits sending it in the clear after security activation. By refusing to respond to an unprotected Identity Request after NAS security was established, the UE correctly adhered to the 3GPP security requirements, thereby protecting subscriber privacy and resisting potential downgrade or interception attacks. Therefore, the UE's action in this scenario was 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 security test, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an Identity Request message for the IMEI in plain (unencrypted) NAS, rather than a protected message. The UE did not respond to this plain Identity Request. According to the 3GPP 5G standard (TS 24.501), once NAS security is established (after Security Mode Complete), the UE must only accept and respond to NAS messages that are integrity protected and, where required, ciphered. If the AMF sends a plain (unencrypted and unprotected) NAS message after security activation, the UE is expected to ignore it for security reasons, as responding could expose sensitive information (such as the IMEI) to interception or replay attacks. Therefore, the UE's action of not responding to the unprotected Identity Request is in line with the 3GPP security requirements and demonstrates secure behavior. Secure
202	202	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.15091204643249512 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15117597579956055 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE requesting the SUCI, but crucially, this message was sent in plain (unencrypted) form, despite the expectation that all subsequent NAS messages should be protected after security activation. The UE did not respond to this unprotected identity request. According to the 3GPP 5G standard (TS 24.501), after the security context is established and security mode is complete, the UE must only accept NAS messages that are integrity protected and, if required, encrypted. By refusing to respond to a plain (unprotected) identity request after security activation, the UE is correctly following the 5G security specifications and protecting against potential security threats such as identity interception or replay attacks. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure

203	203	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15087509155273438 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15108299255371094 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Security Mode Complete message, indicating that NAS security (i.e., 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 GUTI (Globally Unique Temporary Identifier). The UE did not respond to this plain Identity Request. According to the 3GPP 5G standard (TS 24.501), once NAS security is established (after Security Mode Complete), all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, encrypted. The UE is expected to ignore or silently discard any NAS messages received in plain form after security activation, as responding to such messages could expose sensitive information to potential attackers. Therefore, the UE's action of not responding to the unprotected Identity Request is compliant with the 5G security standard and demonstrates secure behavior. Secure
204	204	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15074801445007324 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15094995498657227 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE requesting the IMEISV, but crucially, this message was sent in plain (unencrypted) form. According to 3GPP 5G standards (TS 24.501), once NAS security is established, the UE is required to only respond to NAS messages that are integrity protected and, where applicable, encrypted. If the AMF sends a plain (unencrypted) identity request after security activation, the UE should not respond to this message, as responding would risk exposing sensitive information (such as the IMEISV) over an unprotected channel. In this test, the UE did not respond to the plain identity request, demonstrating correct and secure behavior as per the 3GPP standard. The UE's refusal to respond to an unprotected request after security activation upholds the security of its identity information and aligns with best practices for 5G NAS security. 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 and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the preceding NAS security procedures had been completed. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) NAS. The UE did not respond to this request. According to the 3GPP 5G standard, after the completion of 5G-AKA and establishment of NAS security, all subsequent NAS messages, especially those involving sensitive information such as subscriber identity (SUCI or SUPI), must be protected by NAS security (i.e., encrypted and integrity protected). The UE is expected to ignore or reject any requests for sensitive information received in plain NAS after security has been established, as responding would risk exposing subscriber identity information. 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 3GPP standard and demonstrates secure behavior in this context. 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 key agreement 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, specifically requesting the SUCI (Subscription Concealed Identifier). Notably, this identity request was sent in plain (unencrypted) NAS signaling, even though the 5G-AKA procedure had already been completed, which means that NAS security (encryption and integrity protection) should have been activated at this point. The UE, upon receiving this plain (unencrypted) identity request after security activation, did not respond to the AMF. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated post-authentication, the UE must only accept and respond to NAS messages that are integrity protected and, where required, encrypted. Any subsequent plain NAS messages should be ignored to prevent potential security vulnerabilities such as interception or replay attacks. Therefore, the UE's action of not responding to the unprotected identity request is compliant with the 5G security standards and demonstrates secure behavior in this context. Secure

207	207	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 2.019134998321533 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.0193519592285156 AMF to UE SACK (Ack=7, Arwnd=106361) , DownlinkNASTransport, Identity request 3.000807046890259 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, indicating that the security context had been established and NAS security should now be active. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted) NAS, despite the security context being available. According to 3GPP 5G standards (TS 24.501), once 5G-AKA is complete and the security context is established, all subsequent NAS messages—especially those involving sensitive identifiers like SUCI—must be protected with NAS security (i.e., encrypted and integrity protected). The UE, upon receiving an unprotected identity request after security activation, correctly did not respond, as replying to an unprotected request could expose sensitive information and violate the security requirements of the standard. Therefore, the UE's action of not responding to the unprotected identity request was in line with 3GPP security guidelines and demonstrates secure behavior. Secure
208	208	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4989509582519531 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.49918699264526367 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context should have been established 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 SUCI (Subscription Concealed Identifier) from the UE. The UE did not respond to this request. According to the 3GPP 5G security standards, once 5G-AKA is completed and security context is established, the UE is required to only accept and respond to NAS messages that are integrity protected and, where applicable, encrypted. If the AMF sends a plain (unencrypted) NAS message after security activation, the UE should ignore or silently discard it to prevent potential security risks such as interception or replay attacks. The UE's lack of response to the plain "Identity Request" message is therefore in strict compliance with the 3GPP security requirements, as responding to such a message would have been insecure. Thus, the UE's behavior in this scenario was secure. Secure

209	209	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.48286890983581543 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.48304104804992676 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "registration complete" message to the AMF, indicating that the security context had been established and NAS security should be active. Subsequently, the AMF sent an "identity request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted) NAS format. According to the 3GPP 5G standard, once 5G-AKA is complete and a security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where appropriate, encrypted to prevent exposure of sensitive information and to protect against various attacks. The UE, upon receiving an unprotected (plain) identity request after security activation, took no action and did not respond. This behavior aligns with the 3GPP security requirements, as the UE is expected to ignore or reject any NAS messages that are not properly protected after security activation, especially those requesting sensitive identifiers like the SUCI. By refusing to respond to an insecure request, the UE prevented potential exposure of its identity and adhered to the security principles of the standard. Therefore, the UE's action in this scenario was secure. Secure
210	210	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.48984408378601074 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4900491237640381 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that mutual authentication and key establishment had been achieved. Subsequently, the AMF sent an "Identity Request" message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) NAS signaling. The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed and security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The SUCI is a privacy-sensitive identifier, and the standard mandates that it must not be sent in cleartext after security activation. By refusing to respond to an identity request sent in plain NAS after security activation, the UE is adhering to the 3GPP security requirements and protecting the subscriber's privacy. Therefore, the UE's action in this scenario is correct and secure according to the 5G standard. Secure

211	211	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 4.666033029556274 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originating) 4.666288137435913 AMF to UE SACK (Ack=20, Arwnd=106429) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context had been established and NAS messages should henceforth be protected (i.e., encrypted and integrity protected). Subsequently, the AMF sent an "Identity Request" message requesting the TMSI from the UE, but crucially, this message was sent in plain (unencrypted) text. According to 3GPP standards (TS 24.501), once the security context is established following 5G-AKA, all subsequent NAS messages between the UE and AMF must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unprotected) NAS message after security activation, is required by the standard to discard the message and not respond, as responding to such a message could expose sensitive information and create a security vulnerability. In this test, the UE did not respond to the plain "Identity Request," which is the correct and secure behavior as per 3GPP specifications. Therefore, the UE's action was secure and compliant with the 5G standard. Secure
212	212	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.7599759101867676 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.7602298259735107 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. The AMF then responded with a Downlink NAS Transport message containing an Identity Request for the IMEISV, and crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards (TS 33.501), after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where possible, encrypted. Furthermore, the standard specifies that the UE should not respond to identity requests (such as IMEISV) sent in plain text after security has been activated, as this could expose sensitive information to potential interception. In this test, the UE did not respond to the plain (unencrypted) identity request for the IMEISV, which aligns with the security requirements of the 5G standard and demonstrates proper protection of sensitive information. Therefore, the UE's action was secure. Secure

213	213	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.7595288753509521 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.7598080635070801 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. The AMF then responded with a NAS Identity Request message, requesting the SUCI (Subscription Concealed Identifier) from the UE. Notably, this Identity Request was sent in plain (unencrypted) NAS, even though the 5G-AKA had already been completed, which means that both the UE and the network should have established NAS security context and thus should be able to exchange NAS messages securely (i.e., encrypted and integrity protected). According to 3GPP TS 24.501, once 5G-AKA is completed and a security context is established, all subsequent NAS messages, including identity requests, must be sent with security protection. The UE, upon receiving a plain (unencrypted) Identity Request after security context establishment, correctly did not respond, as responding to an unprotected identity request after authentication would violate 5G security procedures and could expose sensitive information. This behavior aligns with the 3GPP standard, which mandates that the UE should only respond to protected NAS messages after security activation. Therefore, the UE's action in this scenario was secure and in compliance with the 5G standard. Secure
214	214	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.7997701168060303 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.8000459671020508 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, initiating a PDU session establishment request. In response, the AMF sent an Identity Request message to the UE, specifically requesting the TMSI, and this message was sent in plain (unencrypted) form. The UE, upon receiving this plain Identity Request after authentication had already been completed, did not respond. According to the 3GPP 5G security standards (TS 33.501), after the 5G-AKA procedure is completed and security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The UE is expected to ignore or silently discard any NAS messages received in plain (unencrypted) form after security activation, as responding to such messages could expose sensitive information to potential attackers. Therefore, the UE's action of not responding to the plain Identity Request after security activation aligns with the 5G security requirements and demonstrates secure behavior. Secure

215	215	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.5246391296386719 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5248539447784424 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5249319076538086 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF. The AMF then responded with an Identity Request message, specifically requesting the IMEISV, and this message was sent in plain (unencrypted) form. The UE did not respond to this request. According to the 3GPP 5G security standards (TS 33.501), after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where confidentiality is required, encrypted. Sensitive information such as the IMEISV should not be transmitted in plain text after security has been activated. The UE's refusal to respond to a plain (unencrypted) Identity Request for IMEISV after 5G-AKA is completed aligns with the 3GPP security requirements, as responding would expose sensitive information over an unprotected channel. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure
216	216	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.5509819984436035 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5512139797210693 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5513119697570801 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Identity Request message to the UE, specifically requesting the SUCI (Subscription Concealed Identifier). Notably, this Identity Request was sent in plain (unencrypted) NAS, despite the fact that the 5G-AKA procedure—which establishes NAS security—had already been completed. According to the 3GPP 5G security standards (TS 33.501), once NAS security has been established following 5G-AKA, all subsequent NAS messages, especially those involving sensitive information such as identity requests and responses, must be protected (i.e., integrity protected and ciphered). The UE, upon receiving an unprotected (plain) Identity Request after security context establishment, correctly did not respond, as responding to such a request could expose sensitive information and would violate the security requirements of the standard. Therefore, the UE's action demonstrates compliance with 3GPP security guidelines and protects against potential security threats, such as identity interception or replay attacks. Secure

217	217	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.531268835067749 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5314879417419434 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5316059589385986 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF issued an Identity Request message, specifically requesting the IMEISV, and sent this message in plain (unencrypted) form. The UE did not respond to this request. According to the 3GPP 5G security standards (TS 33.501), once the 5G-AKA procedure is completed, NAS signaling messages exchanged between the UE and the AMF must be integrity protected and, where possible, encrypted. Sensitive information such as the IMEISV should not be transmitted in plain text after security has been activated, as this could expose the UE to privacy and security risks (e.g., IMEISV catching attacks). By refusing to respond to an unprotected Identity Request after security activation, the UE is adhering to the 3GPP security requirements and protecting its sensitive identity information. Therefore, the UE's action in this scenario is secure and compliant with the 5G standard. Secure
218	218	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 13.027754783630371 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 13.028036832809448 AMF to UE SACK (Ack=11, Arwnd=106361) , DownlinkNASTransport, Configuration update command 13.02815294265747 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Identity Request message to the UE, specifically requesting the TMSI (Temporary Mobile Subscriber Identity). Notably, this Identity Request was sent in plain (unencrypted) NAS signaling, despite the fact that 5G-AKA had already been completed, which means that NAS security (encryption and integrity protection) should have been activated for all subsequent NAS messages according to 3GPP standards (TS 33.501 and TS 24.501). The UE, upon receiving this unprotected Identity Request, did not respond. This behavior aligns with 3GPP security requirements, which specify that after security mode is established, the UE must ignore any NAS messages not protected by NAS security. By refusing to respond to an unprotected identity request after 5G-AKA completion, the UE prevented potential exposure of sensitive information (such as TMSI) over an unprotected channel, thereby adhering to the security standards. Therefore, the UE's action was secure and compliant with 3GPP 5G security procedures. Secure

219	219	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.5992319583892822 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5994939804077148 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a plain (unencrypted) Identity Request message asking for the TMSI. According to the 3GPP 5G security standards, once 5G-AKA is completed, NAS signaling messages between the UE and the AMF should be integrity protected and, where possible, encrypted to prevent exposure of sensitive information and to resist various attacks. The AMF's choice to send the Identity Request in plain text after authentication is a deviation from the standard, but the focus here is on the UE's behavior. The UE, upon receiving a plain (unencrypted) Identity Request after security context establishment, did not respond. This behavior aligns with 3GPP security requirements, which state that the UE should not respond to NAS messages that are not integrity protected after security activation, as responding could expose sensitive information or make the UE vulnerable to attacks such as replay or man-in-the-middle. By refusing to respond to the unprotected Identity Request, the UE demonstrated secure behavior in accordance with the 5G security 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, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Downlink NAS Identity Request message requesting the TMSI. Notably, the AMF sent this Identity Request as a plain (unencrypted) message, even though the security context should have been established after 5G-AKA completion. According to the 3GPP 5G security standards (TS 33.501 and TS 24.501), once the NAS security context is established (i.e., after 5G-AKA), all subsequent NAS messages, including identity requests, must be integrity protected and, if confidentiality is enabled, encrypted. The UE, upon receiving a plain (unencrypted) Identity Request after security activation, is required by the standard to ignore the message and not respond, in order to prevent possible security attacks such as replay or interception of sensitive information. In this test, the UE did not respond to the plain Identity Request, which is the correct and secure behavior as per 3GPP specifications. Therefore, the UE's action demonstrates compliance with the 5G security requirements and protects against potential security vulnerabilities. Secure

221	221	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 8.961992025375366 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.962584972381592 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is a standard step to request access to network services. The AMF, under test control, responded with a Service Accept message, but crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security specifications (TS 33.501), once 5G-AKA is completed, both the UE and the network are required to establish NAS security, which includes encryption and integrity protection of subsequent NAS messages. The Service Accept message, being a critical NAS message, should have been protected by NAS security. The UE, upon receiving a plain (unencrypted) Service Accept message after security context establishment, is expected to reject or ignore the message, as accepting or responding to unprotected NAS messages after security activation would expose the UE to potential security threats such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected Service Accept message, which aligns with the 3GPP security requirements and demonstrates that the UE correctly enforced the security policy by not accepting unprotected NAS messages after authentication and security activation. Therefore, the UE's action was secure. 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, the 5G-AKA authentication procedure was completed successfully, which means that both the UE and the AMF should have established security contexts for subsequent NAS message protection (integrity and encryption). After authentication, the UE sent a service request to the AMF, and the AMF responded with a service accept message. However, the service accept message from the AMF was sent in plain (unencrypted) form, which is not compliant with 3GPP 5G security standards. According to 3GPP TS 33.501, after successful 5G-AKA and establishment of NAS security, all subsequent NAS messages (including service accept) must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) service accept message after security context establishment, should have rejected the message or at least not acted upon it, 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 provided no response to the plain service accept message, which indicates that it did not accept or process the insecure message. This behavior aligns with the security requirements of the 5G standard, as the UE did not compromise its security by accepting an improperly protected message. Therefore, the UE's action in this scenario was secure. Secure

223	223	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 1.0053770542144775 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.0059680938720703 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a Service Request message to the AMF, which is the expected behavior to initiate a service. In response, the AMF sent a Service Reject message with 5GMM Cause 9 ("UE identity cannot be derived by the network"), and crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards (TS 33.501), after the completion of 5G-AKA, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted to ensure confidentiality and prevent security breaches. The UE, upon receiving a plain (unencrypted) Service Reject message after security context establishment, did not respond further. This behavior aligns with the 3GPP security recommendations, which state that the UE should ignore or not act upon unprotected NAS messages once a security context is in place, as processing 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 adherence to the 5G security requirements and is considered secure behavior. Secure
224	224	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 0.9605340957641602 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.9612541198730469 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which was then followed by the AMF sending a Service Reject message with 5GMM Cause 9 ("UE identity cannot be derived by the network"). Notably, the Service Reject message from the AMF was sent in plain (unencrypted) NAS, even though the 5G-AKA procedure had already been completed, which should have established NAS security. According to the 3GPP 5G standard (TS 24.501), once NAS security is established, the UE is required to only accept further NAS messages that are integrity protected and, if applicable, ciphered. The UE, in this case, did not respond to the unprotected Service Reject message, which aligns with the 3GPP security requirements; the UE should ignore any NAS messages that are not integrity protected after security mode is active. This behavior prevents potential security attacks, such as replay or spoofing, by ensuring the UE does not act on unauthenticated messages. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure

225	225	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.7581770420074463 UE to AMF UplinkNASTransport, Service request 0.7587769031524658 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is the expected behavior to initiate or resume a session. The AMF, under test control, responded with a Service Reject message, which was sent in plain (unencrypted) NAS signaling, and included a 5GMM cause value of 111 (Protocol error, unspecified). According to 3GPP TS 24.501, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, if possible, ciphered (encrypted). The Service Reject message from the AMF was sent in plain text, which is a violation of the standard, but since the AMF was under test control, the focus is on the UE's response. The UE, upon receiving the unprotected Service Reject message, did not respond further. This is the correct and secure behavior as outlined by 3GPP, which specifies that the UE must ignore unprotected NAS messages that require integrity protection after security activation, and must not process or act upon them. By not responding to the unprotected Service Reject, the UE demonstrated compliance with the standard and protected itself from potential security risks such as replay or injection attacks. Secure
226	226	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 21 UE provided: No response The packet capture during the test using wireshark is: 0.7632501125335693 UE to AMF UplinkNASTransport, Service request 0.7634460926055908 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Service reject (Synch failure) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is the expected behavior to initiate a service. In response, the AMF sent a Service Reject message with 5GMM Cause 21 (indicating "synchronization failure") as a plain (unencrypted) NAS message. According to 3GPP TS 24.501, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where possible, encrypted. The UE, upon receiving a plain (unencrypted) Service Reject message after security context establishment, did not respond to the message. This behavior aligns with the 3GPP security requirements, which specify that the UE must ignore any unprotected NAS messages received after security activation, as these could be attempts at NAS message replay or injection attacks. By not responding to the unprotected Service Reject, the UE demonstrated compliance with the standard and protected itself from a potential security vulnerability. Therefore, the action taken by the UE was secure. Secure

227	227	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03d2 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.5453281402587891 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5457210540771484 AMF to UE SACK (Ack=7, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5461199283599854 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Security Mode Command. The Security Mode Command was sent as a protected message, indicating that it was encrypted and integrity protected using the negotiated cipher (5G-EA6) and integrity (128-5G-IA2) algorithms. However, the UE did not respond to the Security Mode Command, and the security header in the downlink message was marked as "Unknown." According to the 3GPP 5G standard, after 5G-AKA, the AMF initiates the NAS security procedure by sending a Security Mode Command to the UE, which the UE must process and respond to with a Security Mode Complete message. The UE should only accept a Security Mode Command that is properly protected and matches the negotiated security algorithms. In this case, since the Security Mode Command was protected and the UE did not respond, it suggests that the UE either did not recognize the security header or detected an anomaly and refused to proceed, which is a secure behavior as per the standard. The UE's refusal to respond to an unknown or potentially malformed security-protected message helps prevent possible security breaches or downgrade attacks. Therefore, the UE's action in this scenario was secure. Secure

228	228	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00f2 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 2.722198963165283 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.7225029468536377 AMF to UE SACK (Ack=8, Arwnd=106361) , DownlinkNASTransport, Configuration update command 2.722743034362793 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the UE proceeds with NAS signaling. The AMF then responded with a Security Mode Command, which is used to establish NAS security by selecting ciphering and integrity protection algorithms. However, the Security Mode Command from the AMF specified both ciphering (5G-EA0) and integrity (5G-IA0) algorithms as "null," meaning no encryption or integrity protection was applied to subsequent NAS messages. Additionally, the security header in the message was marked as "Unknown," and the UE did not respond to this Security Mode Command. According to 3GPP 5G standards, after 5G-AKA, the UE should only accept Security Mode Commands that require at least integrity protection (and typically ciphering as well, unless local policy dictates otherwise). Accepting null algorithms would leave NAS signaling unprotected, exposing the UE to security risks such as eavesdropping and message tampering. The UE's lack of response to the Security Mode Command with null algorithms aligns with the 3GPP security requirements, as the UE is expected to reject or ignore insecure security configurations. Therefore, the UE's action in this scenario was secure, as it did not proceed with unprotected NAS communication. Secure
229	229	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.8296740055084229 UE to AMF UplinkNASTransport, Service request 0.8299529552459717 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a standard step to resume or establish a NAS signaling connection. The AMF then responded with a Configuration Update Command, but crucially, this downlink NAS message was sent in plain (unencrypted and unauthenticated) form, as indicated by the security header value of 0 (Plain NAS message). According to the 3GPP 5G standards, specifically TS 24.501, once 5G-AKA is completed and NAS security is established, all subsequent NAS messages exchanged between the UE and the AMF must be protected by both integrity and ciphering (i.e., they must not be sent in plain). The UE, upon receiving a plain (unprotected) NAS message after security context establishment, is required by the standard to discard the message and not respond, as a security measure to prevent potential attacks or tampering. In this test, the UE did not respond to the unprotected Configuration Update Command, which aligns with the 3GPP security requirements and demonstrates correct, secure behavior by the UE. Therefore, the UE's action was secure. Secure

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

231	231	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3100 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 5G-IA5 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.4284870624542236 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4289300441741943 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4293291568756104 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is a normal step in NAS communication. The AMF then responded with a Security Mode Command message, but notably, this message was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standards (TS 24.501), after successful authentication (5G-AKA), the Security Mode Command is used to establish NAS security (ciphering and integrity protection) between the UE and the AMF. However, the Security Mode Command itself is always sent as a plain message, since security context is not yet established at this point. The UE is expected to respond with a Security Mode Complete message, which will be the first NAS message protected with the negotiated security algorithms. In this test, the UE did not respond to the Security Mode Command. This lack of response is not compliant with the 3GPP standard, as the UE should have accepted the security context and replied accordingly. The absence of a response could indicate a security issue, such as the UE refusing to proceed with security context establishment, or a malfunction. Therefore, based on the standard and the expected behavior, the UE's action was insecure, as it failed to establish NAS security and proceed with the secure communication as required. Insecure
232	232	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.7425761222839355 UE to AMF UplinkNASTransport, Service request 0.7428131103515625 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a standard step to resume or establish a session. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) NAS signaling. According to the 3GPP 5G security standards (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where possible, encrypted. An Authentication Reject message sent in plain text after authentication is a protocol anomaly and could be a potential attack vector (e.g., a downgrade or denial-of-service attack). The UE, upon receiving an unprotected Authentication Reject after security context establishment, is expected to ignore the message and not respond, as processing such a message could compromise security. In this test, the UE did not respond to the plain Authentication Reject, which aligns with the 3GPP security recommendations and demonstrates proper handling of protocol violations. Therefore, the UE's action was 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 the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a standard step to resume or establish a session. The AMF, under test control, responded with an Authentication Reject message, which was sent in plain (unencrypted) NAS signaling. According to the 3GPP 5G security standards (TS 33.501), once 5G-AKA is completed, NAS security (encryption and integrity protection) should be activated for all subsequent NAS messages, except for a few specific cases (such as initial registration or authentication procedures themselves). The Service Request message from the UE was sent after 5G-AKA, so it should have been protected, and the UE should expect all subsequent NAS messages to be protected as well. Upon receiving an unprotected (plain) Authentication Reject message after security context establishment, the UE correctly provided no response. This behavior aligns with 3GPP security guidelines, which state that the UE must ignore unprotected NAS messages that should be protected, as responding to such messages could expose the UE to security risks such as replay or downgrade attacks. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure
234	234	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.1599588394165039 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.160261869430542 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE completed the initial NAS steps and sent an authentication response to the AMF, the AMF responded with an identity request for the TMSI, sent as a plain (unencrypted) NAS message. At this point, the 5G-AKA procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established between the UE and the AMF. According to the 3GPP 5G standard, the UE should not respond to identity requests sent in plain NAS after the authentication response, as this could expose sensitive information (such as the TMSI) to interception by an attacker, especially in the case of a rogue AMF or man-in-the-middle attack. The UE's lack of response to the plain identity request indicates that it correctly refused to send potentially sensitive information before NAS security was activated, thereby adhering to the security requirements specified by 3GPP. This behavior demonstrates that the UE is protecting user identity information as required by the standard. **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 procedures and sent an authentication response to the AMF, the AMF responded with an identity request for the IMEISV. Importantly, this identity request was sent as a plain (unencrypted) NAS message because the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard (TS 24.501), the UE is required to protect its permanent identifiers, such as the IMEI or IMEISV, and should not transmit them in plain text over the air. The standard specifies that the UE should only respond to identity requests for permanent identifiers after NAS security has been activated, unless there is no other option (e.g., for emergency services). In this test, the UE did not respond to the AMF's plain (unencrypted) request for the IMEISV, which aligns with the security requirements of 3GPP to avoid exposing sensitive identifiers before a secure channel is established. Therefore, the UE's action demonstrates adherence to the 5G security standard and protects the subscriber's privacy by not transmitting the IMEISV in the clear. Secure
236	236	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0173 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.15990495681762695 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1602330207824707 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3627040386199951 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then responded with a Security Mode Command. Notably, the Security Mode Command was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), after the completion of 5G-AKA, all subsequent NAS messages that carry sensitive information, such as the Security Mode Command, should be integrity protected and, if possible, ciphered. The UE, upon receiving a plain Security Mode Command after authentication, responded with a Deregistration Request, effectively refusing to proceed with further communication under insecure conditions. This behavior aligns with the 3GPP security requirements, which specify that the UE must not accept or process security-related NAS messages unless they are properly protected after authentication is complete. By refusing to proceed and deregistering, the UE demonstrated correct and secure behavior in accordance with the standard, thereby protecting itself from potential security risks such as replay or man-in-the-middle attacks. Secure

237	237	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 5G- IA0 (null) Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.12820696830749512 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12850189208984375 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which is the expected behavior. Subsequently, the AMF sent a Security Mode Command to the UE, initiating the NAS security context. The Security Mode Command was protected, indicating that it was integrity protected and/or ciphered as per the security context established during 5G-AKA. However, the AMF specified the use of ciphering algorithm 5G-EA5 and the null integrity algorithm 5G-IA0, meaning that while the NAS messages would be encrypted, there would be no integrity protection (i.e., no way for the UE to verify that the message was not tampered with). The security header was marked as unknown, and the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard, it is a security requirement that integrity protection must be enabled for NAS signaling to prevent attacks such as message tampering or replay. If the network proposes a null integrity algorithm (5G-IA0), the UE is permitted—and in fact expected—to reject the Security Mode Command or not respond, as accepting such a configuration would expose the UE to security risks. Therefore, the UE's lack of response to a Security Mode Command that did not provide integrity protection is consistent with secure behavior as defined by the 3GPP standard, as it avoids establishing a vulnerable security context. Secure
238	238	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03967404365539551 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.03995108604431152 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF. Subsequently, the AMF sent another Identity Request message to the UE, specifically requesting the TMSI, and this message was sent in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to 3GPP 5G security standards, sensitive information such as permanent or long-term identifiers (e.g., SUPI/IMSI) should not be transmitted in plain text before the establishment of a secure NAS security context, which is achieved after 5G-AKA completion. However, temporary identifiers like the TMSI are designed to be used in such situations to protect the subscriber's permanent identity. In this case, the UE did not respond to the AMF's plain Identity Request for the TMSI. This behavior aligns with a conservative security posture, as the UE avoided transmitting even a temporary identifier in the clear before security activation, possibly due to strict implementation or additional security checks. Given that the 5G-AKA was not completed and the message was sent in plain text, the UE's refusal to respond can be considered secure, as it minimizes the risk of exposing any identifying information over an unprotected channel, even if only a temporary identifier was requested. 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.	During the test, after completing the initial NAS procedures, the UE sent an Identity Response to the AMF. Subsequently, the AMF issued another Identity Request, specifically requesting the IMEISV, and this message was sent in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standards, sensitive information such as the IMEISV should not be transmitted over the air in plain text before a secure NAS security context is established (i.e., after 5G-AKA is completed and NAS security is activated). In this scenario, the UE did not respond to the AMF's plain (unencrypted) Identity Request for the IMEISV, which aligns with the security requirements to prevent exposure of sensitive identifiers before encryption is in place. This behavior demonstrates that the UE is adhering to the 3GPP security guidelines by refusing to send sensitive information in an unprotected manner, thus maintaining the confidentiality of the IMEISV. Secure
240	240	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0363 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.12767410278320312 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1279001235961914 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Authentication Response to the AMF, which is the expected behavior. Subsequently, the AMF issued a Security Mode Command to the UE, but this command was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), after the completion of authentication, the Security Mode Command is the mechanism by which the AMF instructs the UE to activate NAS security (encryption and integrity protection) for subsequent messages. The UE is required to verify the integrity and authenticity of the Security Mode Command before responding. If the Security Mode Command is received as a plain NAS message after authentication, the UE must treat this as a potential security risk, since an attacker could inject or modify such messages. The correct and secure behavior for the UE, as per the standard, is to ignore or reject plain Security Mode Commands after authentication is complete, and not to respond to them. In this test, the UE did not respond to the plain Security Mode Command, which aligns with the 3GPP security requirements and demonstrates that the UE is protecting itself against potential attacks or protocol misuse. Therefore, the UE's action was secure. Secure

241	241	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.16009092330932617 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1604149341583252 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was completed, establishing the necessary security context for protected NAS communication between the User Equipment (UE) and the Access and Mobility Management Function (AMF). Following this, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security algorithms (ciphering: 5G-EA7, integrity: 128-5G-IA2). However, after this step, the AMF sent another "security mode command" message, which is not expected according to the 3GPP 5G NAS protocol flow; the security mode command should only be sent once per registration or security context establishment. The UE, upon receiving this unexpected and protected security mode command, did not respond. According to 3GPP standards, the UE should ignore or silently discard any further security mode command messages received after the security mode has already been completed, as responding to such messages could indicate a vulnerability to replay or downgrade attacks. The UE's lack of response demonstrates correct and secure behavior, as it did not process or acknowledge a potentially malicious or erroneous command, thereby adhering to the security requirements of 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 test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which is the expected behavior as per the 3GPP 5G security procedures. Subsequently, the AMF sent a Security Mode Command to the UE, which is used to establish NAS security (ciphering and integrity protection) for subsequent messages. The Security Mode Command was sent as a protected message, indicating that it was integrity protected (and possibly ciphered) using the negotiated algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity). However, the UE did not respond to the Security Mode Command. According to the 3GPP standard, upon receiving a Security Mode Command, the UE must verify the integrity of the message and, if valid, respond with a Security Mode Complete message to confirm the establishment of NAS security. The absence of any response from the UE suggests that it either failed to process the Security Mode Command or chose not to respond, which is not compliant with the standard and could indicate a security or implementation issue. By not responding, the UE avoids establishing NAS security, which is a critical step for protecting subsequent NAS messages. Therefore, the action taken by the UE in this scenario is considered insecure as it does not fulfill the required security procedures outlined by 3GPP for 5G standalone operation. Insecure

243	243	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0293 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.15967893600463867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.15994000434875488 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then replied with a Security Mode Command. Notably, the Security Mode Command was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), it is expected and required that the Security Mode Command message is sent as a plain NAS message, since at this point, the NAS security context has not yet been established; the Security Mode Command itself is used to set up the NAS security context (i.e., to agree on ciphering and integrity algorithms). The UE, upon receiving the Security Mode Command in plain text, is expected to respond with a Security Mode Complete message, which should be the first NAS message protected with the newly established security context. However, in this test, the UE did not respond at all to the Security Mode Command. This lack of response could indicate that the UE rejected the plain Security Mode Command, which would be non-compliant with the 3GPP standard, as the UE is supposed to accept and process a plain Security Mode Command after successful authentication. If the UE failed to respond because it expected the Security Mode Command to be encrypted, this would be a misunderstanding of the standard and could cause interoperability issues. Therefore, based on the 3GPP standard, the UE's action in not responding to a correctly formatted plain Security Mode Command after 5G-AKA is considered insecure, as it does not comply with the expected behavior and could prevent successful establishment of secure communications. Insecure

244	244	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0033 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.16002106666564941 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602630615234375 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the security algorithms and parameters negotiated during the security mode command. However, the AMF then sent another "security mode command" message to the UE, but this message was transmitted as a plain (unencrypted and unauthenticated) NAS message, even though the security context had already been established. According to the 3GPP 5G standard, once the security context is in place (i.e., after 5G-AKA and the initial security mode command/complete exchange), all subsequent NAS messages between the UE and the AMF must be integrity protected and, if ciphering is enabled, encrypted. The UE, upon receiving a plain security mode command after security activation, did not respond to this message. This behavior aligns with the 3GPP standard, which mandates that the UE should ignore any plain NAS messages that require security protection once a security context is active, to prevent downgrade or replay attacks. Therefore, the UE's action of not responding to the insecure, plain security mode command was correct and secure according to the 5G standard. Secure
245	245	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15975403785705566 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16004419326782227 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the IMEISV, but this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), sensitive information such as the IMEISV should not be transmitted in the clear before NAS security (encryption and integrity protection) is established, which only occurs after successful completion of 5G-AKA. The UE, upon receiving a plain identity request for the IMEISV before security activation, did not respond. This behavior aligns with the security recommendations in the standard, which state that the UE should not disclose permanent or sensitive identifiers (like IMEISV) over an unprotected channel to prevent potential interception by attackers. Therefore, the UE's refusal to respond to the unprotected identity request demonstrates secure behavior as per 3GPP guidelines. Secure

246	246	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.11967587471008301 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11993288993835449 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the TMSI, sent in plain (unencrypted) NAS message format. At this stage, the 5G-AKA procedure had not yet been completed, which means that NAS security context (encryption and integrity protection) had not been established between the UE and the AMF. According to the 3GPP 5G standard (TS 24.501), the UE should not respond to identity requests that are sent in plain NAS after the authentication response, as this could expose sensitive information (such as the TMSI or SUPI) to potential interception or replay attacks. The UE's action of not responding to the plain identity request after authentication response aligns with the security requirements of the standard, as it prevents the disclosure of potentially sensitive identifiers before a secure context is established. Therefore, the UE's behavior in this scenario was secure and compliant with 3GPP security guidelines. Secure
247	247	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.1999650001525879 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.20019102096557617 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the IMEISV, but crucially, this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA procedure had not yet been completed. According to 3GPP 5G security standards (TS 33.501), sensitive identifiers such as the IMEISV should only be transmitted after a secure NAS signaling connection has been established, which requires the successful completion of the 5G-AKA authentication and key agreement procedure. Since the AMF requested the IMEISV before security activation, the UE was correct in not responding to this request, as sending the IMEISV in plain text would expose the UE to privacy risks such as device tracking or identity theft. Therefore, the UE's action aligns with 3GPP security requirements by refusing to transmit sensitive information over an unprotected channel. Secure

248	248	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA3 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.11875295639038086 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11905193328857422 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was successfully completed between the UE and the AMF, establishing the necessary security context for subsequent NAS message protection. After the UE sent an Authentication Response, the AMF responded with a Security Mode Command, which, according to the test summary, was sent as a "Protected" message using the specified cipher (128-5G-EA2) and integrity (128-5G-IA3) algorithms. However, the security header of the message was marked as "Unknown," and the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA, the Security Mode Command is the first message that should be integrity protected but not ciphered, as ciphering is only activated after the Security Mode Complete message from the UE. If the Security Mode Command was sent as a protected (ciphered and/or integrity protected) message before the security context was fully activated, the UE should reject or ignore the message as per the standard, since it cannot yet process ciphered NAS messages. The UE's lack of response indicates that it did not process the Security Mode Command, which aligns with secure behavior as defined by the 3GPP standard, preventing potential security vulnerabilities from premature ciphering or integrity protection. Therefore, the UE's action in this scenario was secure. Secure
249	249	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.7274200916290283 UE to AMF UplinkNASTransport, Service request 0.7277319431304932 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a typical step to resume or establish a connection. In response, the AMF sent a Configuration Update Command to the UE, but crucially, this downlink NAS message was sent in plain (unencrypted) format, as indicated by the security header value of 0. According to the 3GPP 5G standard, after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted to ensure confidentiality and prevent tampering or eavesdropping. The UE, upon receiving a plain (unencrypted) NAS message after security context establishment, is expected to reject the message or ignore it, 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 plain Configuration Update Command, which aligns with the security requirements of the 3GPP standard by refusing to process an insecure message after security activation. Therefore, the UE's action in this scenario was secure. Secure

250	250	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03999590873718262 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040209054946899414 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an identity response to the AMF. Subsequently, the AMF sent another identity request, specifically requesting the IMEISV, and this message was sent in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standards, sensitive information such as the IMEISV should only be transmitted after a secure NAS security context has been established, which occurs after successful completion of 5G-AKA. Since the UE did not respond to the AMF's plain (unencrypted) request for the IMEISV, it correctly refused to send sensitive information over an insecure channel, adhering to the security requirements outlined by 3GPP. This behavior demonstrates that the UE is properly implementing the standard's security measures by not exposing sensitive identifiers before encryption is in place. Secure
251	251	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03961300849914551 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039839982986450195 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response message to the AMF, and subsequently, the AMF issued another Identity Request message, specifically requesting the TMSI, which was sent as a plain (unencrypted) NAS message because the 5G-AKA authentication procedure had not yet been completed. The UE, upon receiving this plain Identity Request, did not respond. According to the 3GPP 5G security standards, particularly TS 33.501, the UE is required to protect its permanent and sensitive identities (such as SUPI) and should not respond to identity requests for sensitive information over unprotected (plain) NAS messages after the initial registration steps, unless specifically allowed by the standard. By refusing to respond to a plain Identity Request for the TMSI before the establishment of a secure NAS context (i.e., before 5G-AKA completion), the UE is adhering to the security principle of not exposing potentially sensitive identifiers over an unprotected channel. This behavior helps prevent possible identity disclosure attacks and aligns with the security requirements of the 5G standard. 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, the 5G standalone User Equipment (UE) completed the initial NAS steps and sent an identity response to the Access and Mobility Management Function (AMF). Following this, the AMF, under tester control, sent another identity request to the UE, specifically requesting the IMEISV (International Mobile Equipment Identity and Software Version). Importantly, this identity request was sent in plain (unencrypted) NAS signaling, as the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed and thus no security context was established. The UE did not respond to this identity request. According to the 3GPP 5G security standards (TS 33.501), sensitive information such as the IMEISV should not be transmitted over unprotected NAS signaling; instead, the UE is expected to withhold such information until a secure context is established, unless explicitly permitted by the standard. By refusing to respond to the unprotected identity request for the IMEISV, the UE demonstrated correct and secure behavior, adhering to the 5G security requirements and protecting its sensitive information from potential interception. Therefore, the UE's action in this scenario was secure. Secure
253	253	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.7599589824676514 UE to AMF UplinkNASTransport, Service request 0.7601721286773682 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a standard step for resuming or establishing a NAS signaling connection. In response, the AMF sent an Identity Request message, specifically requesting the UE's GUTI (Globally Unique Temporary Identifier). Notably, this Identity Request was sent in plain (unencrypted) NAS signaling, despite the fact that 5G-AKA had already been completed and security context should have been established. According to the 3GPP 5G security standards (TS 33.501), once the security context is in place after 5G-AKA, all subsequent NAS messages—including identity requests—must be integrity protected and, where applicable, encrypted. The UE, upon receiving an unprotected (plain) Identity Request after security activation, did not respond. This behavior aligns with the 3GPP standard, which mandates that the UE must ignore any NAS messages that are not properly protected once security is established, to prevent potential security breaches such as identity theft or replay attacks. Therefore, the UE's refusal to respond to the unprotected Identity Request demonstrates correct and secure behavior as per the 5G standard. Secure

254	254	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 6.647611856460571 UE to AMF SACK (Ack=7, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 6.6478259563446045 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is the expected behavior as the UE initiates a PDU session establishment request. The AMF then responded with a Downlink NAS Transport message containing a Service Accept, but crucially, this message was sent in plain (unencrypted) text. According to the 3GPP 5G security standards (TS 33.501), after the completion of 5G-AKA, NAS security (encryption and integrity protection) must be activated before any further NAS messages are exchanged, except for a very limited set of messages (such as Security Mode Command/Complete). The Service Accept message is not among those exceptions and should be protected. The UE, upon receiving an unprotected (plain) Service Accept message after security activation, did not respond. This behavior aligns with the 3GPP standard, which expects the UE to discard or ignore unprotected NAS messages that should have been secured after security activation. Therefore, the UE's action—providing no response to an unprotected Service Accept—demonstrates secure behavior as per the 5G standard. Secure
255	255	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 12.160748958587646 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 12.161019086837769 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a normal step to request access to network services. The AMF then responded with an Identity Request message, specifically requesting the IMEI, but crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards (TS 33.501), after 5G-AKA is completed, all subsequent NAS messages that could reveal sensitive information, such as the IMEI, must be protected by NAS security (i.e., integrity protected and ciphered). The UE, upon receiving an unprotected Identity Request for the IMEI after security context establishment, did not respond. This behavior aligns with the 3GPP security requirements, as the UE is expected to reject or ignore requests for sensitive information that are not properly protected after authentication and security mode setup. Therefore, the UE's refusal to respond to an unprotected request for its IMEI demonstrates adherence to the 5G security standard and protects the user's privacy. Secure

256	256	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 97 UE provided: No response The packet capture during the test using wireshark is: 0.46838808059692383 UE to AMF UplinkNASTransport, Registration complete 0.4686100482940674 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Message type non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context should have been established. Subsequently, the AMF sent a "GMM Status" message with cause 97 ("Message type non-existent or not implemented") as a plain (unencrypted and unauthenticated) NAS message. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (after 5G-AKA), all subsequent NAS messages, except for a very limited set (such as Service Request and Deregistration Request/Accept under specific conditions), must be integrity protected and, if possible, encrypted. Sending a "GMM Status" message in plain NAS after security activation is not compliant with the standard, and the UE is expected to ignore such messages to prevent potential security risks, such as replay or injection attacks. In this test, the UE did not respond to the plain "GMM Status" message, which aligns with the 3GPP security requirements and demonstrates that the UE correctly rejected an insecure message that could have been exploited by an attacker. Therefore, the UE's behavior was secure in this interaction. Secure
257	257	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4328169822692871 UE to AMF UplinkNASTransport, Registration complete 0.4330179691314697 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication and security procedures, the UE sent a "registration complete" message to the AMF, indicating that the initial NAS security context had been established. Subsequently, the AMF sent an "identity request" message to the UE, requesting the SUCI (Subscription Concealed Identifier). Notably, this identity request message was sent in plain (unencrypted) NAS, despite the fact that security should have been activated after 5G-AKA completion. The UE, upon receiving this unprotected identity request, did not respond. According to the 3GPP 5G standard (TS 24.501), once the security context is established (i.e., after 5G-AKA), the UE must only respond to NAS messages that are integrity protected and ciphered; it should ignore or silently discard any subsequent plain (unencrypted) NAS messages that request sensitive information, such as the SUCI. The UE's refusal to respond to the unprotected identity request aligns with this security requirement, as responding to such a request could expose sensitive subscriber information to potential interception or replay attacks. Therefore, the UE's action in this scenario was in accordance with the 5G standard and demonstrated secure behavior. Secure

258	258	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Plain Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.4842751026153564 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4844861030578613 AMF to UE SACK (Ack=13, Arwnd=106401) , DownlinkNASTransport 2.688286066055298 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the registration process had finished. The AMF, under test control, then sent a "Deregistration Request" message to the UE. Notably, this downlink message from the AMF was sent as "Plain" (i.e., not encrypted), but with the security header indicating "Integrity protected and ciphered (2)", which is inconsistent because a message cannot be both plain and encrypted. Following this, the UE responded with a "Deregistration Request (UE originating)" message. According to the 3GPP 5G security standards, after 5G-AKA is completed, all subsequent NAS messages between the UE and AMF must be both integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The UE, upon receiving a deregistration request that was not properly protected (sent as plain), should have rejected or ignored the message rather than responding to it, as processing unprotected NAS messages after security activation can expose the UE to security risks such as replay or downgrade attacks. Therefore, the UE's action of responding to an improperly protected deregistration request is not compliant with 3GPP security requirements and is considered insecure behavior. Insecure
259	259	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 99 UE provided: No response The packet capture during the test using wireshark is: 0.5207638740539551 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.521324872970581 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Information element non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which is expected to be encrypted and integrity protected as per 3GPP standards once authentication is complete. The AMF, under test control, responded with a GMM Status message indicating a 5GMM Cause value of 99 ("Information element non-existent or not implemented"), and crucially, this message was sent in plain (unencrypted) form. According to 3GPP TS 24.501, after security activation (i.e., after 5G-AKA), the UE should only accept NAS messages that are both integrity protected and ciphered; any plain (unencrypted) NAS messages received after security activation should be discarded and not responded to. In this test, the UE did not respond to the plain GMM Status message from the AMF, which aligns with the security requirements of the 3GPP standard, as responding to or processing unprotected messages after security activation could expose the UE to security risks such as replay or modification attacks. Therefore, the UE's action—specifically, providing no response to the unprotected message—demonstrates correct and secure behavior as per the 5G 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 completing 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 have been established and all subsequent NAS messages should be integrity protected and ciphered. However, the AMF then sent a "5GMM Status" message with cause 101 ("Message not compatible with the protocol state") as a plain (unencrypted and non-integrity protected) message. Upon receiving this plain message, the UE responded with a "Deregistration Request (UE originating)" message. According to the 3GPP 5G standards (TS 24.501), after security activation, the UE must ignore any NAS messages received in plain format unless they are allowed exceptions (such as Service Reject or Deregistration Accept). The 5GMM Status message is **not** one of these exceptions and must be integrity protected and ciphered after security mode is complete. By responding to a plain, unprotected 5GMM Status message with a deregistration request, the UE failed to comply with the security requirements, as it should have ignored the unprotected message instead of acting upon it. This behavior exposes the UE to potential security risks, such as denial-of-service attacks or protocol downgrades, if an attacker injects plain NAS messages. Therefore, the UE's action in this scenario is not secure according to the 5G standard. Insecure
261	261	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0101 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.7511579990386963 UE to AMF UplinkNASTransport, Service request 0.7514059543609619 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request by sending an UplinkNASTransport message to the AMF. In response, the AMF sent a Security Mode Command as a downlink message, which was indicated as "Protected" and included the ABBA parameter, ciphering algorithm 128-5G-EA1, and integrity algorithm 128-5G-IA2. However, the security header of the message was marked as "Unknown," and the UE did not provide any response to the Security Mode Command. According to the 3GPP 5G standard, after 5G-AKA, the Security Mode Command is used to establish NAS security (ciphering and integrity protection) for subsequent NAS messages. The UE is expected to process this command and respond with a Security Mode Complete message if the command is valid and properly protected. The lack of response from the UE suggests that it either did not recognize the Security Mode Command as valid, did not trust the protection, or encountered an error in processing the message. This cautious behavior by the UE—refusing to proceed without a valid and recognizable security header—aligns with the security principles outlined in the 3GPP standard, as it prevents the establishment of NAS security under potentially insecure or ambiguous conditions. Therefore, the UE's action in this scenario can be considered secure. Secure

262	262	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 8.914944887161255 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.915573835372925 AMF to UE SACK (Ack=13, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. The AMF responded with a Security Mode Command, which was sent as a plain (unencrypted and unauthenticated) NAS message, specifying the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm. The UE did not respond to this Security Mode Command. According to the 3GPP 5G standard (TS 24.501), after authentication, the Security Mode Command is used to establish NAS security, and it is permissible for the initial Security Mode Command to be sent in plain text. However, the use of the null ciphering algorithm (5G-EA0) means that subsequent NAS messages would not be encrypted, only integrity protected. The UE's lack of response to the Security Mode Command in this context is a secure behavior, as accepting a null ciphering algorithm could expose subsequent NAS messages to eavesdropping. Therefore, the UE's refusal to proceed with insecure security parameters aligns with 3GPP security requirements and best practices. Secure
263	263	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 74 UE provided: No response The packet capture during the test using wireshark is: 0.5198588371276855 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5200669765472412 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Registration reject (Temporarily not authorized for this SNPN) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message (specifically a PDU session establishment request) to the AMF. In response, the AMF sent a Registration Reject message with 5GMM Cause 74 ("Temporarily not authorized for this SNPN"). Notably, this Registration Reject message was sent in plain (unencrypted) NAS, even though 5G-AKA had already been completed, which means that NAS security context should have been established and all subsequent NAS messages (except for a few exceptions defined in 3GPP TS 24.501, such as certain reject messages before security activation) should be integrity protected and, where applicable, encrypted. According to the 3GPP standard, after 5G-AKA, the UE is expected to only accept NAS messages that are integrity protected (and, if required, encrypted). In this test, the UE did not respond to the plain Registration Reject message, indicating that it did not accept or process an unprotected message after security context establishment. This behavior is compliant with the 3GPP security requirements, as accepting unprotected NAS messages after security activation would expose the UE to security risks such as spoofing or denial-of-service attacks. Therefore, the UE's action—refusing to process the unprotected Registration Reject message—was secure and in line with 5G security standards. 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 the UE continues its registration and session establishment process. Subsequently, the AMF responded with a Registration Reject message, indicating a 5GMM cause value of 6 ("Illegal ME"), and this message was sent in plain (unencrypted) form. According to the 3GPP 5G standards (TS 24.501), after the completion of 5G-AKA, NAS security (encryption and integrity protection) should be activated for all subsequent NAS messages exchanged between the UE and the AMF. The UE, upon receiving a plain Registration Reject message after security has been established, is expected to discard the message and not act upon it, as accepting unprotected messages at this stage could expose the UE to security risks such as spoofing or denial-of-service attacks. In this test, the UE did not respond to the unprotected Registration Reject message, which demonstrates correct and secure behavior in line with 3GPP requirements. The UE's refusal to process or respond to an unprotected NAS message after security activation ensures the integrity and confidentiality of its communication and protects it from potential security threats. Secure

265	265_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1111 RAND: 0e38a634245d3e4aea72a7f7a7148161 AUTN: 3d9033e57f3e8000d3eb278394dd7c46 ngKSI_TSC: Native security context ngKSI_KSI: 5 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 1.0084679126739502 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.0087080001831055 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Authentication request 1.216444969177246 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF sent an Authentication Request message in plain (unencrypted) form, reusing the same ngKSI (Key Set Identifier) as previously established during the 5G-AKA procedure. The UE responded with an Authentication Failure message, specifically indicating "ngKSI already in use." According to the 3GPP 5G security standards, once a native security context is established and 5G-AKA is completed, the AMF should not initiate a new authentication procedure with the same ngKSI, nor should it send authentication requests in plain text when a security context is already in place. The UE's action to reject the authentication request and report the reuse of ngKSI is compliant with 3GPP security requirements, as it prevents potential replay or downgrade attacks and ensures that the established security context is not compromised. By refusing to process a redundant or potentially malicious authentication request, the UE maintains the integrity and confidentiality of the communication as required by the standard. Therefore, the UE's behavior in this scenario is secure. Secure
266	266	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.5199589729309082 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.520190954208374 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. In response, the AMF sent an Authentication Reject message in plain (unencrypted) NAS format. According to the 3GPP 5G security standards, after 5G-AKA is completed, NAS security (encryption and integrity protection) should be activated, and all subsequent NAS messages, including error or reject messages, must be protected. The UE, upon receiving a plain (unencrypted) Authentication Reject message after security context establishment, did not respond. This behavior aligns with 3GPP TS 24.501, which specifies that the UE must ignore any unprotected NAS messages that require integrity protection after security has been activated. By not responding to the unprotected Authentication Reject, the UE demonstrated correct and secure behavior, as responding to or accepting such a message could expose it to security risks such as spoofing or denial of service attacks. Therefore, the UE's action in this scenario was secure. 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 a UL NAS Transport message to the AMF, which was then followed by the AMF sending an Authentication Reject message in plain (unencrypted) form. According to the 3GPP 5G standards, once 5G-AKA is completed, both the UE and the network are expected to establish NAS security, meaning that subsequent NAS messages should be integrity protected and, where required, encrypted. The Authentication Reject message is a security-critical message because it can trigger the UE to delete security contexts and prevent further network access. The 3GPP standard (TS 24.501) mandates that after security mode is established, the UE should only accept certain messages, including Authentication Reject, if they are integrity protected, and should ignore or silently discard such messages if they are received in plain (unencrypted and unprotected) form. In this test, the UE did not respond to the plain Authentication Reject message sent by the AMF after security was established, which aligns with the 3GPP security requirements and demonstrates that the UE is not vulnerable to a potential security downgrade or denial-of-service attack via unauthenticated messages. Therefore, the UE's action in this scenario was secure. Secure
268	268	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.7500498294830322 UE to AMF UplinkNASTransport, Registration complete 0.7504808902740479 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and security procedures, the UE sent a "Registration Complete" message to the AMF, indicating that it had finished the registration process. Following this, the AMF sent a "Configuration Update Command" message to the UE, which was marked as "Protected" but had an "Unknown" security header. Notably, the UE did not respond to this message. According to the 3GPP 5G standards (TS 24.501), after security activation, all subsequent NAS messages between the UE and AMF must be integrity protected and, where required, ciphered. If a message is received with an unknown or invalid security header, the UE is expected to discard the message and not respond, as a security measure to prevent potential attacks or protocol violations. The UE's lack of response in this scenario indicates that it correctly identified the message as potentially insecure or malformed and took the appropriate action by not processing or acknowledging it. This behavior aligns with the security requirements of the 5G standard, demonstrating that the UE acted securely in this interaction. Secure

269	269	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.46799302101135254 UE to AMF UplinkNASTransport, Registration complete 0.4681861400604248 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context should have been established and subsequent NAS messages should be protected (i.e., integrity protected and ciphered) as per 3GPP TS 33.501 and TS 24.501. However, the AMF then sent a "Deregistration Accept" message to the UE in plain (unencrypted and non-integrity protected) form, which is a deviation from the standard, as all NAS messages after security activation must be protected. The UE, upon receiving this unprotected NAS message, did not respond. According to 3GPP specifications, the UE is required to discard any NAS message received in plain format after security has been activated and should not process or respond to such messages. The UE's lack of response indicates that it correctly identified the security anomaly and acted in accordance with the standard by not accepting or acknowledging the unprotected message. Therefore, the UE's behavior in this scenario was secure and compliant with 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 procedures, the UE sent an identity response to the AMF. Subsequently, the AMF sent another identity request, specifically requesting the IMEISV, and this message was transmitted in plain (unencrypted) NAS, as the 5G-AKA authentication and key agreement had not yet been completed. According to 3GPP standards (TS 33.501), sensitive information such as the IMEISV should not be transmitted in plain text after the security context is established; however, before 5G-AKA is completed, the NAS messages are not yet encrypted, and the UE is expected to protect its identity information as much as possible. In this case, the UE did not respond to the AMF's plain (unencrypted) request for the IMEISV, which aligns with the security principle of minimizing exposure of sensitive information when encryption is not yet established. This cautious behavior by the UE demonstrates adherence to security best practices as outlined by 3GPP, as it avoids sending sensitive identifiers in the clear before a secure context is in place. Therefore, the UE's action in not responding to the unprotected identity request is considered secure. Secure

271	271	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.03961491584777832 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.03991198539733887 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response message to the AMF. Subsequently, the AMF sent another Identity Request, specifically requesting the IMEI, and this message was sent in plain (unencrypted) form because the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G security standards, sensitive information such as the IMEI should not be transmitted in plaintext before the NAS security context is established (i.e., before 5G-AKA is completed and NAS messages are encrypted). The UE, upon receiving a plaintext Identity Request for the IMEI before security activation, did not respond. This behavior aligns with 3GPP security recommendations, which state that the UE should not disclose permanent or device identities (like IMEI) over unprotected NAS signaling to prevent potential interception by attackers. Therefore, the UE's refusal to respond to the unprotected IMEI request demonstrates secure and standards-compliant behavior. Secure
272	272	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007159709930419922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept 0.2011561393737793 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a Service Accept message that was marked as "Protected" (i.e., integrity protected and/or encrypted). However, the critical step of 5G-AKA (Authentication and Key Agreement) was not completed prior to this exchange. According to the 3GPP 5G security architecture, NAS message protection (encryption and integrity) can only be applied after successful completion of 5G-AKA, which establishes the necessary security context and keys. Since 5G-AKA was not completed, the UE should not have accepted or processed a "Protected" NAS message, nor should it have proceeded to send further messages (such as a Deregistration Request) in response to a protected message, as the required security context was not established. The UE's action of accepting a protected Service Accept message and then responding with a Deregistration Request indicates a deviation from the 3GPP security procedures, potentially exposing the UE to security risks such as replay or spoofing attacks. Therefore, based on the 3GPP standard, the UE's behavior in this scenario was insecure. 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, indicating it was participating in the 5G-AKA authentication process. However, before the 5G-AKA procedure was completed (i.e., before security context establishment), the AMF sent a Deregistration Request to the UE. Notably, this Deregistration Request was sent as a protected message, with the security header indicating both integrity protection and ciphering. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) should only be applied after the successful completion of the 5G-AKA procedure, when both the UE and the AMF have established a shared security context. Since the 5G-AKA was not yet completed, the UE should not have been able to decrypt or verify the integrity of the protected message, and therefore, it is correct and secure for the UE to provide no response to this message. This behavior prevents potential security vulnerabilities, such as accepting or acting on messages that appear protected but cannot be verified due to the absence of a security context. Therefore, the UE's action in this scenario aligns with 3GPP security requirements and demonstrates secure behavior. Secure
274	274	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.11959981918334961 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1198418140411377 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent its authentication response to the AMF, the AMF immediately sent a deregistration request message to the UE. Notably, the 5G-AKA authentication procedure was not yet completed, meaning that the mutual authentication and the establishment of NAS security (encryption and integrity protection) had not been finalized. Despite this, the AMF sent the deregistration request as a "protected" message, with the NAS security header indicating integrity protection. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) should only be applied after successful completion of the 5G-AKA procedure, when security keys have been established. Since the UE had not yet completed authentication and therefore had not derived the necessary security keys, it would not be able to verify or decrypt protected messages. The UE, in this case, did not respond to the protected deregistration request, which is the correct and secure behavior as per the standard, because processing a protected message without established security context could expose the UE to security risks such as replay or spoofing attacks. Therefore, the UE's action of not responding to the prematurely protected message was secure and compliant with 3GPP requirements. Secure

275	275	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007669925689697266 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal ME) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. At this stage, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that security context establishment (i.e., mutual authentication and derivation of encryption/integrity keys) had not occurred. Despite this, the AMF responded with a DownlinkNASTransport message containing a Deregistration Request, which was sent as a protected (integrity protected and ciphered) NAS message. According to the 3GPP 5G standard, NAS message protection (integrity protection and ciphering) can only be applied after the security context is established via 5G-AKA. Since the UE had not yet completed 5G-AKA, it would not possess the necessary keys to decrypt or verify the integrity of the protected message. The UE, therefore, did not respond to the AMF's protected Deregistration Request, which is the correct and secure behavior as per the standard; responding to a message it cannot authenticate or decrypt could expose the UE to security risks such as replay or downgrade attacks. In summary, the UE's action of not responding to a protected NAS message before security context establishment aligns with 3GPP security requirements and demonstrates secure behavior. 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 the described test scenario, the UE completed the initial NAS procedures and sent an Identity Response to the AMF. The AMF then sent a Security Mode Command to the UE as a plain (unencrypted and unauthenticated) NAS message, indicating that the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G standards, specifically TS 33.501, the Security Mode Command must be sent as a plain NAS message because the NAS security context is not yet established prior to the completion of 5G-AKA. However, the UE is required to verify that the Security Mode Command is received in the correct sequence and only after successful authentication. Since the 5G-AKA was not completed, the UE did not respond to the Security Mode Command, which aligns with the security requirements to prevent potential security breaches such as downgrade or replay attacks. The UE's refusal to proceed with security mode setup before authentication ensures that it does not establish security contexts with an unauthenticated network entity, thereby protecting itself from possible attacks. Based on this behavior, the UE acted securely and in compliance with the 3GPP standard. Secure

277	277	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.04006814956665039 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040535926818847656 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response message to the AMF. Immediately following this, the AMF sent a Configuration Update Command to the UE. Notably, this downlink message from the AMF was sent with a security header indicating integrity protection, but the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) must only be applied after successful completion of the 5G-AKA procedure, as this is when the necessary security context is established. Since the AMF sent a protected message before 5G-AKA was completed, the UE, adhering to the standard, did not respond to this message because it could not verify its integrity or decrypt it without the established security context. This behavior by the UE demonstrates compliance with the 3GPP security requirements, as it avoids processing potentially unauthenticated or malicious messages before security is in place. Therefore, the UE's action in this scenario was secure. Secure
278	278	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.3110721111297607 UE to AMF UplinkNASTransport, Identity response 2.311551094055176 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Configuration update command 2.3115811347961426 UE to AMF SACK (Ack=3, Arwnd=106437) , UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, which then replied with a Configuration Update Command sent as a plain (unencrypted) NAS message, since the 5G-AKA authentication and key agreement had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), NAS messages should only be sent in plain text prior to the completion of 5G-AKA, after which all subsequent NAS messages must be integrity protected and, where applicable, encrypted. Upon receiving a plain Configuration Update Command before security activation, the UE did not process the command but instead responded with a Deregistration Request, effectively terminating the session. This behavior is in line with 3GPP security requirements, which expect the UE to reject or ignore any configuration or sensitive commands received in plain text after the point where security should be activated, or if such commands are received before security activation in a suspicious context. The UE's refusal to process the plain Configuration Update Command and its subsequent deregistration demonstrate a secure and standards-compliant response to a potentially insecure situation. Secure

279	279	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007669925689697266 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a deregistration accept message, which was sent as a protected (integrity-protected and/or ciphered) NAS message. However, the 5G-AKA authentication procedure, which is required to establish NAS security (encryption and integrity protection), had not yet been completed at this point in the exchange. According to the 3GPP 5G standard, the UE should not process or respond to protected NAS messages before the 5G-AKA procedure is completed and security context is established, as the cryptographic keys necessary for protection are not yet in place. In this test, the UE did not respond to the protected deregistration accept message sent by the AMF before security establishment, which is the correct and secure behavior as per the standard. This prevents potential security vulnerabilities such as accepting or acting on messages that could be spoofed or manipulated before mutual authentication and key agreement. Therefore, the UE's action in this scenario was secure. Secure
280	280	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007870197296142578 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. However, before the 5G-AKA authentication and key agreement procedure was completed—which is required to establish security context and enable encryption and integrity protection for NAS messages—the AMF responded with a deregistration accept message. Notably, this downlink message was sent as "protected," even though the security context had not yet been established. The UE, upon receiving this protected deregistration accept message, did not respond further. According to the 3GPP 5G standard, NAS message protection (encryption and integrity) can only be applied after successful completion of the 5G-AKA procedure, as this is when the necessary keys are derived. If the UE receives a protected NAS message before security context is established, it should ignore or silently discard the message, as it cannot verify its integrity or decrypt it. The UE's lack of response indicates that it correctly followed the 3GPP security requirements by not processing a protected message before security context was established, thus preventing a potential security vulnerability. Therefore, the UE's action in this scenario was secure. Secure

281	281	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00080108642578125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test, the UE initiated a 5G standalone registration by sending an unprotected initial registration request to the AMF, as expected before security establishment. The AMF, under test control, responded with a configuration update command that was integrity protected and ciphered using a new security context, even though the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G standard, security procedures such as integrity protection and ciphering should only be applied after successful completion of 5G-AKA, which establishes the necessary security context between the UE and the network. Since the UE did not respond to the protected configuration update command (sent before 5G-AKA completion), it correctly refused to process a message that was protected with a security context that had not yet been established. This behavior aligns with 3GPP security requirements, as the UE must not accept or process protected NAS messages before mutual authentication and key agreement are completed. Therefore, the UE's action in this scenario was secure. Secure
282	282	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006248950958251953 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated the NAS communication by sending an initial registration request to the AMF. At this point, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that security context establishment (integrity and ciphering keys) between the UE and the AMF was not yet in place. Despite this, the AMF responded with a Configuration Update Command message that was integrity protected and ciphered, as indicated by the security header (2). According to the 3GPP 5G standard, the UE should only accept and process NAS messages that are protected (integrity protected and/or ciphered) after the security context has been established via successful completion of 5G-AKA. Since the 5G-AKA was not completed, the UE correctly did not respond to the protected Configuration Update Command, thereby avoiding processing a message that should not have been protected at this stage. This behavior aligns with the 3GPP security requirements, as it prevents potential security vulnerabilities such as replay or downgrade attacks. Therefore, the UE's action in this scenario was secure. Secure

283	283	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006029605865478516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an initial registration request to the AMF, which is the expected behavior at the start of NAS communication. However, the 5G-AKA authentication procedure, which is required to establish security context and enable NAS message encryption and integrity protection, had not yet been completed. Despite this, the AMF sent a "service accept" message to the UE, and this message was marked as "protected" (i.e., encrypted or integrity protected). According to the 3GPP 5G standards, NAS message protection (encryption and integrity) must not be applied until after successful completion of the 5G-AKA procedure and establishment of security context between the UE and the AMF. The UE, upon receiving a protected NAS message before security context establishment, is expected to discard the message and not respond, as it cannot decrypt or verify the integrity of the message. In this test, the UE did not respond to the protected "service accept" message sent before 5G-AKA completion, which is the correct and secure behavior as per 3GPP standards. The UE's action ensured that it did not process or acknowledge potentially spoofed or out-of-sequence protected messages before security was established. 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 standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a DownlinkNASTransport carrying a Service Accept message, which was marked as "Protected" (i.e., integrity protected and/or encrypted). However, the 5G-AKA authentication procedure, which establishes security keys for NAS message protection, had not yet been completed. According to 3GPP standards (TS 33.501 and TS 24.501), NAS message protection (encryption and integrity) must only be applied after successful completion of 5G-AKA, when both the UE and the network have derived the necessary security context. Since the UE received a "Protected" Service Accept message before security activation, it should have recognized this as a protocol violation and rejected the message or deregistered, as it cannot verify the protection without established keys. The UE's action—sending a Deregistration Request immediately after receiving the improperly protected message—demonstrates correct and secure behavior according to the 3GPP standard, as it did not proceed with unverified or potentially malicious communication. This indicates the UE properly enforced the security requirements of the 5G standard. Secure

285	285	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.039772987365722656 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Plmn not allowed) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an identity response to the AMF, which is a plain (unencrypted) message as expected before security activation. However, the AMF then sent a deregistration request to the UE with the security header indicating that the message was both integrity protected and ciphered (i.e., encrypted and authenticated). According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) can only be applied after the successful completion of the 5G-AKA authentication and key agreement procedure, which establishes the necessary security context. In this test, the 5G-AKA was not completed, so the UE had not yet established the keys required to decrypt or verify the protected message from the AMF. The UE did not respond to the protected deregistration request, which is the correct and secure behavior according to the standard, as it should ignore any NAS messages requiring security before security context is established. Therefore, the UE's action was secure and fully compliant with the 3GPP 5G specifications. 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, after the UE initiated the registration procedure by sending an initial registration request to the AMF, the AMF responded with a GMM status message containing a 5GMM Cause value of 98 ("Message type not compatible with the protocol state"). Notably, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that NAS security context (encryption and integrity protection) was not yet established between the UE and AMF. According to 3GPP standards (TS 24.501), before the completion of 5G-AKA and the establishment of a NAS security context, the UE should not accept or process protected (i.e., encrypted or integrity-protected) NAS messages, as it does not yet possess the necessary keys. In this test, the AMF sent a protected GMM status message, and the UE did not respond to it. This behavior aligns with the 3GPP standard, as the UE correctly ignored a protected message received before security context establishment, thereby preventing potential security vulnerabilities such as replay or spoofing attacks. Therefore, the UE's action in this scenario was secure. 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 registration by sending an initial registration request to the AMF, but the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. The AMF, under test control, responded with a protected (i.e., integrity-protected and/or encrypted) GMM status message indicating a 5GMM cause of 3 ("Illegal UE"). According to the 3GPP 5G standard, the UE should only process protected NAS messages after the 5G-AKA procedure is completed and NAS security is established; before this, the UE should ignore or discard any protected NAS messages, as it cannot verify their integrity or decrypt them. In this test, the UE did not respond to the protected GMM status message sent by the AMF before security was established, which is the correct and secure behavior as per 3GPP standards. By not responding, the UE avoided processing potentially spoofed or malicious messages before a secure context was set up, thus protecting itself from certain attacks. Secure
288	288	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0008118152618408203 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.20334196090698242 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an Initial Registration Request to the AMF. The AMF responded with a Security Mode Command, which was protected with integrity using the 128-5G-IA2 algorithm but did not use ciphering (5G-EA0, the null ciphering algorithm). Importantly, the Security Mode Command was sent before the completion of the 5G-AKA authentication procedure, meaning that the security context was not yet fully established and ciphering was not enabled. Upon receiving this, the UE responded with a 5GMM status message indicating "Invalid mandatory information," which suggests the UE detected an issue with the received Security Mode Command—likely because it was sent with integrity protection and a new security context before the proper authentication (5G-AKA) was completed. According to the 3GPP 5G standards, the security context (including the selection and activation of ciphering and integrity algorithms) should only be established after successful authentication. The UE's action to reject or flag the message as invalid demonstrates adherence to the standard and a correct security posture, as it did not proceed with establishing security based on an incomplete or invalid context. Therefore, the UE's behavior in this scenario was secure and compliant with 3GPP requirements. Secure

289	289	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 6.12048602104187 UE to AMF SACK (Ack=5, Arwnd=106496) , UplinkNASTransport, Identity response 6.120656967163086 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication where, after completing the initial NAS steps, the UE responded to an identity request by sending an Identity Response. Subsequently, the AMF sent another Identity Request, specifically requesting the GUTI, and this message was sent in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. The UE, upon receiving this second plain Identity Request, did not respond. According to the 3GPP 5G security standards, sensitive information such as the GUTI should not be transmitted in plain text after the initial registration steps, especially before the security context is established via 5G-AKA. The UE's refusal to respond to a plain (unencrypted) identity request for the GUTI is consistent with the security requirements, as it prevents potential exposure of sensitive identifiers to eavesdroppers. Therefore, the UE's action demonstrates adherence to the 5G security standard by not disclosing the GUTI in an unprotected message. Secure
290	290	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.039791107177734375 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040058135986328125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an identity response to the AMF. Subsequently, the AMF issued another identity request, specifically asking for the IMEISV, and this message was sent in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standards, sensitive information such as the IMEISV should not be transmitted in plaintext before the establishment of a secure NAS connection, which is achieved only after successful 5G-AKA completion. The UE, upon receiving a plaintext identity request for the IMEISV before security activation, chose not to respond. This behavior aligns with 3GPP security recommendations, which state that the UE should not disclose sensitive identifiers like the IMEISV over an unprotected channel to prevent potential interception or misuse. Therefore, the UE's refusal to respond to the unprotected identity request demonstrates adherence to security best practices as defined by the standard. Secure

291	291	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03981208801269531 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04005002975463867 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, after which the AMF sent another Identity Request, specifically requesting the TMSI, in plain (unencrypted) NAS signaling. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to 3GPP standards (TS 33.501 and TS 24.501), the UE should not send sensitive identifiers such as the TMSI or SUPI in response to plain (unencrypted) NAS messages after the initial identity exchange, especially before NAS security is activated. In this test, the UE did not respond to the AMF's subsequent plain Identity Request for the TMSI, which aligns with the security requirements of the 5G standard to prevent exposure of sensitive information over unprotected signaling. Therefore, the UE's action in withholding a response to the unprotected identity request was secure and compliant with 3GPP security guidelines. Secure
292	292	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.11100292205810547 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11120295524597168 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated)(Re-authentication required) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the 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 and Key Agreement) procedure was not yet completed. Immediately after receiving the Authentication Response, the AMF sent a Deregistration Request message to the UE, which was integrity protected (as indicated by the security header), but not encrypted, since encryption is only enabled after successful completion of 5G-AKA. The UE did not respond to this Deregistration Request. According to the 3GPP 5G security standards, the UE should not accept or process NAS messages that are protected (integrity only) but not encrypted, if the security context (i.e., 5G-AKA) has not been established. This is because, prior to the completion of 5G-AKA, the keys required for encryption and integrity protection are not yet derived, and any protected message from the network could be a security risk (e.g., replay or spoofing attacks). By not responding to the Deregistration Request before 5G-AKA completion, the UE correctly avoided processing a potentially insecure message, adhering to the 3GPP security guidelines. Therefore, the UE's action in this scenario was secure. 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 security test scenario, the 5G standalone User Equipment (UE) successfully completed the 5G-AKA authentication procedure, after which it sent a "registration complete" message to the AMF. Following this, the AMF (under tester control) sent a "configuration update command" to the UE as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard, once 5G-AKA is completed and NAS security is established, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. The UE, upon receiving a plain NAS message after security context establishment, is expected to reject or ignore such messages, as accepting or processing them would expose the UE to potential security threats such as spoofing or tampering. In this test, the UE did not respond to the plain "configuration update command" sent by the AMF after security was established, demonstrating correct and secure behavior as per 3GPP specifications. By refusing to process an unprotected message after security activation, the UE effectively protected itself from a potential security breach. Secure
294	294	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 31313131313131313131005fb686550000 AUTN: 3030303030303000ee555fb686550000 ngKSI_TSC: Mapped security context ngKSI_KSI: 2 UE provided: No response The packet capture during the test using wireshark is: 0.11998605728149414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.12024092674255371 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to begin secure NAS communication. However, the AMF subsequently sent an "authentication request" message to the UE in plain (unencrypted) form, despite the fact that, per 3GPP standards, all subsequent NAS messages after the security mode complete should be integrity protected and, if possible, encrypted. The UE, upon receiving this plain (unencrypted) authentication request after security activation, did not respond. According to 3GPP TS 33.501 and TS 24.501, the UE must reject or ignore any NAS messages received in plain format after security has been activated, as accepting or responding to such messages could expose the UE to security risks such as replay or downgrade attacks. Therefore, the UE's action of not responding to the unprotected authentication request is in strict compliance with the 5G security standards, demonstrating secure behavior. 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, the 5G-AKA authentication procedure was completed successfully, establishing the necessary security context for subsequent NAS message encryption and integrity protection. The UE then sent a "security mode complete" message, indicating it accepted the negotiated NAS security algorithms and was ready to communicate securely. Immediately after, the AMF sent a "service reject" message with 5GMM Cause 111 (protocol error, unspecified), but crucially, this message was sent in plain (unencrypted) form. According to 3GPP 5G standards (TS 24.501), after successful completion of the security mode command, all subsequent NAS messages—including reject messages—must be integrity protected and, if required, encrypted. The UE, upon receiving a plain (unencrypted) service reject after security activation, did not respond or process the message. This behavior aligns with 3GPP security requirements, which state that UEs must ignore NAS messages that are not integrity protected after security has been established, to prevent security downgrade or spoofing attacks. Thus, the UE's action of not responding to the unprotected service reject message demonstrates correct and secure behavior 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 accepted the negotiated security algorithms and was ready to proceed with protected NAS communication. However, the AMF, under test control, subsequently sent an "authentication request" message to the UE in plain (unencrypted) form, which is not the expected behavior according to the 3GPP 5G standard. According to 3GPP TS 24.501, once the security mode is completed, all subsequent NAS messages between the UE and AMF must be integrity protected and, if required, ciphered. The UE, upon receiving a plain (unencrypted) authentication request after security mode completion, did not respond. This behavior aligns with the 3GPP specification, which states that the UE should discard any unprotected NAS messages received after security activation, as accepting or responding to such messages could expose the UE to security risks such as replay or downgrade attacks. Therefore, the UE's lack of response demonstrates secure and standards-compliant behavior in this context. Secure

297	297	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.16003108024597168 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16027402877807617 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the next message from the AMF to the UE was a "deregistration accept" sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after the security mode complete), all subsequent NAS messages exchanged between the UE and the AMF must be protected (encrypted and integrity protected). The UE, upon receiving a plain (unencrypted) NAS message after security activation, is required by the standard to discard the message and not respond, as accepting or processing such a message would be a security vulnerability. In this test, the UE did not respond to the unprotected deregistration accept message, which is the correct and secure behavior as per the 3GPP specification. Therefore, the UE's action was secure. Secure
298	298	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.1601550579071045 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16047000885009766 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to establish a secure NAS communication channel. Subsequently, the AMF, under test control, sent an "authentication reject" message to the UE, but crucially, this message was sent in plain (unencrypted) text rather than being protected by the established NAS security context. According to the 3GPP 5G standard (TS 24.501), once the security mode procedure is successfully completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, if required, encrypted. The standard also specifies that the UE should ignore any downlink NAS messages received in plain text after security activation, except for a limited set of messages (such as "security mode command" or "deregister request"), and "authentication reject" is not among these exceptions. In this test, the UE did not respond to the plain "authentication reject" message, which aligns with the 3GPP security requirements, as accepting or acting upon unprotected messages after security activation could expose the UE to security risks such as downgrade or replay attacks. Therefore, the UE's action of ignoring the unprotected message demonstrates correct and secure behavior as per the 5G standard. Secure

299	299	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.15986394882202148 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16010284423828125 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to begin secure NAS communication. Immediately after, the AMF sent an "authentication reject" message to the UE, but this message was sent in plain (unencrypted) form, despite the fact that the security context had already been established. According to the 3GPP 5G standard (TS 24.501), once the security mode is completed and the security context is active, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) NAS message after security activation, is required by the standard to treat this as a potential security breach (such as a replay or downgrade attack) and must not respond to such messages. In this test, the UE did not respond to the plain "authentication reject" message, which aligns with the security requirements of the 5G standard and demonstrates correct, secure behavior in the face of a protocol anomaly. Secure
300	300	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.15969204902648926 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15989899635314941 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. Immediately following this, the AMF sent an "identity request" message to the UE, requesting the TMSI, but crucially, this message was sent in plain (unencrypted) form. The UE did not respond to this plain identity request. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after the security mode complete), the UE must only accept and respond to NAS messages that are integrity protected and, if required, encrypted. Any plain (unencrypted and non-integrity protected) NAS messages received after security activation should be ignored or rejected by the UE to prevent security vulnerabilities, such as identity interception or replay attacks. The UE's refusal to respond to the plain identity request demonstrates adherence to this security requirement, ensuring that sensitive information like the TMSI is not exposed in an unprotected message. Therefore, the UE's action was secure and compliant with the 5G standard. Secure