UE Response Evaluation Report: Test time: 2025-07-17 17:40:36

SL	Test Name	Test content	Remark
1	1	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006918907165527344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. In response, the AMF sent an Identity Request message, specifically requesting the IMEI, and this message was sent in plain (unencrypted) form because the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), sensitive identifiers such as the IMEI should not be transmitted in plain text over the air interface before security has been established, as this could expose the UE to privacy and security risks, such as device tracking or unauthorized identification. In this case, the UE did not respond to the plain (unencrypted) Identity Request for the IMEI, which aligns with the security recommendations of the 3GPP standard to protect device identity information until a secure NAS connection is established. Therefore, the UE's action of withholding its IMEI in the absence of NAS security was appropriate and secure according to the 5G standard. Secure
2	2	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0011980533599853516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2027890682220459 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. In response, the AMF sent an Identity Request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE then replied with an Identity Response containing the requested SUCI. Importantly, this exchange occurred before the completion of the 5G-AKA authentication procedure, meaning that NAS security (encryption and integrity protection) had not yet been established, and the messages were sent in plain (unencrypted) form. According to the 3GPP 5G standard, it is expected and required that the UE provides the SUCI (which is a privacy-preserving, encrypted form of the permanent identifier SUPI) in the clear prior to authentication, as the SUCI is specifically designed to protect the subscriber's identity even when sent over an unprotected channel. Therefore, the UE's action of sending the SUCI in response to a plain Identity Request before 5G-AKA completion is compliant with the 3GPP security requirements and does not expose the permanent identifier (SUPI) to interception. Based on this, the UE's behavior in this scenario is secure. Secure

3	3	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0002651214599609375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as there is not yet a shared key to enable encryption. The UE, upon receiving the Authentication Reject message, did not respond further, which is the expected and secure behavior as per the standard: the UE should abort the registration procedure and not proceed with any further NAS communication when it receives an Authentication Reject. This prevents the UE from exposing itself to further potential attacks or information leakage. Therefore, the UE's action—ceasing communication after receiving a plain Authentication Reject before security context establishment—aligns with 3GPP security requirements and is considered secure. Secure
4	4	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0012979507446289062 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20431208610534668 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. In response, the AMF sent an identity request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE then replied with an identity response containing the requested SUCI. Importantly, this exchange occurred before the completion of the 5G-AKA authentication procedure, meaning that NAS security (encryption and integrity protection) had not yet been established, and the messages were sent in plain (unencrypted) form. According to the 3GPP 5G standard, it is expected and required that the initial registration and identity request/response messages, including the transmission of the SUCI, occur before NAS security is activated, as the network needs to identify the UE before authentication and key agreement can proceed. The SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) by encrypting it, so that even when sent in the clear, the actual SUPI is not exposed. Therefore, the UE's action of sending the SUCI in response to a plain identity request prior to 5G-AKA completion is compliant with the 3GPP security architecture and does not expose sensitive information. Based on this, the UE's behavior in this scenario is secure. 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 this message was sent in plain (unencrypted) form because 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) back to the AMF. According to the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as there is no shared key yet for encryption. The UE's action to send a deregistration request after receiving a registration reject is a standard-compliant and expected behavior, as it is a proper response to being denied registration. There is no indication that the UE accepted or processed any unauthorized or malformed messages, nor did it proceed with any further registration steps without security context. Therefore, based on the 3GPP standard and the sequence of actions, the UE's behavior in this scenario was secure. Secure
6	6	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 22 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0009021759033203125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Congestion) 0.20517516136169434 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a registration reject message (5GMM Cause 22: Congestion) before the 5G-AKA authentication procedure was completed. As a result, the registration reject message was sent in plain (unencrypted) form, which is expected since security context establishment (via 5G-AKA) had not yet occurred. Upon receiving the registration reject, the UE responded with a deregistration request (UE originating), also in plain text, as no security context was available. According to 3GPP standards (TS 24.501), the UE is required to accept and process registration reject messages sent in plain text prior to security activation, and it is also permitted to send subsequent messages (such as deregistration requests) in plain text under these circumstances. The UE's actions—accepting the plain registration reject and responding appropriately—are compliant with the 5G standard and do not introduce any security vulnerabilities, as encryption is not mandated before authentication and key agreement are completed. Therefore, the UE's behavior in this scenario is considered secure according to 3GPP specifications. Secure

7	7	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 00000000000000000000000000000000 AUTN: 32303030007f0000ee555cc720560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007770061492919922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.203125 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an initial registration request to the AMF. In response, the AMF sent an authentication request message to the UE, but this message was sent in plain (unencrypted) form and included suspicious parameters such as an all-zero RAND value and an ABBA value of 0000. Upon receiving this authentication request, the UE responded with an "Authentication failure (Non-5G authentication unacceptable)" message, indicating that it rejected the authentication attempt because it did not conform to 5G authentication requirements. According to the 3GPP 5G standard, the UE must only proceed with authentication if the request is valid and meets the security requirements, including the use of proper cryptographic parameters and, where required, message protection. The UE's refusal to proceed with an insecure or non-standard authentication request demonstrates adherence to the 5G security specifications, as it prevents potential security breaches such as replay or downgrade attacks. Therefore, the UE's action in this scenario was secure and in line with 3GPP standards. 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: 31303030000000000078742b94d4550000 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 initial registration request to the AMF. The AMF, under test control, responded with an authentication request message that was sent in plain (unencrypted) form, with the 5G-AKA authentication procedure not yet completed. The authentication request included a zeroed AUTN and a test RAND value, and the security context was indicated as native but not yet established. Upon receiving this message, the UE did not proceed with authentication but instead responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G security standards, the UE is required to verify the integrity and validity of authentication requests before proceeding, especially when the message is received in plain text and before a security context is established. The UE's action to reject the authentication request due to invalid or missing mandatory information (such as a zeroed AUTN) aligns with the expected secure behavior, as it prevents the UE from proceeding with potentially insecure or spoofed authentication procedures. This response helps protect the UE from possible security attacks, such as replay or man-in-the-middle attacks, that could exploit unprotected NAS messages. Therefore, the UE's behavior in this scenario is consistent with 3GPP security requirements and demonstrates secure handling of the authentication process. Secure

9	9	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03973102569580078 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003596305847168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24200010299682617 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication before the completion of the 5G-AKA authentication procedure, which is required to establish NAS security (encryption and integrity protection). The AMF sent an identity request for the SUCI (Subscription Concealed Identifier), and the UE responded with an identity response. Notably, the AMF sent the identity request as a plain (unencrypted) message, and the UE responded accordingly, also in plain text. According to the 3GPP 5G standard, before 5G-AKA is completed, NAS messages—including identity requests and responses—are permitted to be sent in plain text, as 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, as it is a concealed version of the SUPI. Therefore, the UE's action of responding to a plain identity request with a SUCI in plain text is compliant with the 3GPP standard and does not expose sensitive information. The UE did not send the SUPI or any other sensitive identifier in the clear, and the use of SUCI is specifically intended for this pre-authentication phase. Based on this analysis, the UE's actions were secure and in line with the 5G security requirements. Secure

10	10	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3100 RAND: 313131313131313131006f90d2550000 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 0.039749860763549805 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0399777889251709 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.2409358024597168 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE responded to an identity request from the AMF with an identity response. The AMF then sent an authentication request to the UE, but this request was sent in plain (unencrypted) form, 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, with the ngKSI indicating a native security context and a KSI value of 2. Upon receiving this authentication request, the UE replied with an authentication failure message, specifically stating "ngKSI already in use." According to the 3GPP 5G security standards, the UE should not accept an authentication request that attempts to reuse an ngKSI (NAS key set identifier) that is already in use, as this could indicate a replay or downgrade attack. By refusing to proceed with authentication under these circumstances, the UE is following the security guidelines set by 3GPP to prevent potential security breaches. Therefore, the UE's action in this scenario is considered secure, as it correctly identified and rejected a potentially insecure authentication attempt before any sensitive information could be compromised. 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) completed the initial NAS steps and sent an Identity Response message to the Access and Mobility Management Function (AMF). At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that the security context for NAS message encryption and integrity protection was not yet established. The AMF, under test control, responded with a Service Reject message (5GMM Cause 11: "PLMN not allowed") sent in plain (unencrypted) form. The UE, upon receiving this message, did not respond further. According to the 3GPP 5G standard, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as encryption and integrity protection are only mandated after successful authentication and key agreement. The UE's behavior—sending the Identity Response in plain text and not responding to the Service Reject—aligns with the expected protocol operation and does not expose the UE to additional security risks in this context. Therefore, based on the 3GPP standard and the sequence of events, the UE's actions were secure. Secure

12	12	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03978896141052246 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04010796546936035 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2456059455871582 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 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 responded with another identity response. Notably, 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. According to the 3GPP 5G standard, it is expected and required that identity requests and responses (such as SUCI) can be exchanged in plain (unencrypted) NAS messages prior to the completion of 5G-AKA, as the security context is not yet available. The UE's action of responding to a plain identity request with a plain identity response before 5G-AKA is therefore compliant with the standard and does not represent a security breach, as the SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) even when sent in the clear. Thus, the UE's behavior in this interaction was secure and in line with 3GPP requirements. Secure
13	13	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.03993391990661621 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04019308090209961 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication where, after the initial steps, the UE sent an Identity Response message to the AMF. The AMF, under test control, replied with an Authentication Reject message, which was sent in plain (unencrypted) form. The UE, upon receiving this Authentication Reject, did not respond further. According to the 3GPP 5G standard, NAS messages are only protected (encrypted and integrity protected) after the successful completion of the 5G-AKA authentication procedure. Since the 5G-AKA was not completed in this test, it is expected and compliant for the messages exchanged up to this point—including the Authentication Reject—to be sent in plain text. Furthermore, the UE's lack of response to the Authentication Reject is also in line with the standard, as the UE is expected to abort the registration procedure and not proceed further upon receiving such a message. Therefore, the UE's actions in this scenario were secure and compliant with the 3GPP 5G security requirements. Secure

14	14	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 22 UE provided: No response The packet capture during the test using wireshark is: 0.03981804847717285 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04005002975463867 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Registration reject (Congestion) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). After the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is expected to be sent in plain (unencrypted) form since the 5G-AKA authentication and key agreement procedure had not yet been completed. The AMF, under test control, then sent a Registration Reject message with 5GMM Cause 22 (Congestion), also in plain text, as encryption is not yet established before authentication. The UE, upon receiving the Registration Reject, did not respond further, which aligns with 3GPP standards, as the UE is expected to cease registration attempts upon receiving a reject message. According to the 3GPP 5G security architecture, messages prior to the completion of 5G-AKA (including Identity Response and Registration Reject) are permitted to be sent in plain text, as security context and encryption keys are not yet established. Therefore, the UE's actions—sending the Identity Response in plain text and not responding to the Registration Reject—are consistent with the 5G standard and do not expose the UE to additional security risks in this context. The UE did not take any insecure actions during this exchange. Secure
15	15	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 30303030303030007844783aae550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.03972196578979492 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24048709869384766 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an identity response to the AMF, the AMF replied with an authentication request message that was sent in plain (unencrypted) form, with the 5G-AKA procedure not yet completed. The authentication request included suspicious or invalid parameters, such as an AUTN value of all zeros and a RAND value that does not appear to be random. Upon receiving this, the UE responded with an "Authentication failure (Non-5G authentication unacceptable)" message, indicating that it rejected the authentication attempt because it did not conform to 5G authentication requirements. According to the 3GPP 5G standard, the UE must not accept authentication requests that are not properly protected or that do not follow the expected cryptographic procedures, especially before a secure context is established. The UE's refusal to proceed with authentication under these insecure and non-standard conditions demonstrates adherence to the security requirements of the 5G standard, as it prevents potential downgrade or replay attacks and ensures that sensitive information is not exposed before a secure channel is established. Therefore, the UE's action in this scenario was secure. Secure

16	16	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3200 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 5G-IA7 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.11983895301818848 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12023711204528809 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Authentication Response to the AMF, which is the expected behavior. Subsequently, the AMF sent a Security Mode Command to the UE, but 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), the Security Mode Command is always sent as a plain NAS message because the NAS security context has not yet been established at this point; the purpose of this message is to negotiate and activate NAS security (ciphering and integrity protection) between the UE and the network. The UE, upon receiving this plain Security Mode Command, is expected to process it and respond with a Security Mode Complete message, which will be the first NAS message protected with the newly agreed security algorithms. However, in this test, the UE did not respond to the Security Mode Command at all. This lack of response is not compliant with the 3GPP standard, as the UE is required to respond to a valid Security Mode Command sent in plain text after 5G-AKA. By not responding, the UE is not establishing NAS security, which could leave the communication channel vulnerable if this behavior occurred in a real network. Therefore, the UE's action in this scenario is considered insecure, as it fails to proceed with the required security establishment procedure as defined by the 3GPP standard. Insecure
17	17	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.35177087783813477 UE to AMF UplinkNASTransport, Authentication response 0.35199785232543945 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated NAS communication and, after completing the initial steps, sent an Authentication Response to the AMF. However, before the 5G-AKA authentication procedure was completed, the AMF responded with a Service Reject message, which was sent in plain (unencrypted) text with a 5GMM cause code 111 (Protocol error, unspecified). The UE, upon receiving this unprotected Service Reject message before security context establishment, did not respond further. According to the 3GPP 5G standard, the UE should not accept or act upon critical NAS messages (such as Service Reject) that are received in plain text after the authentication procedure has started but before security has been activated, as this could be exploited by an attacker to disrupt service (e.g., via a "downgrade" or "denial of service" attack). The UE's lack of response to the unprotected Service Reject message demonstrates correct and secure behavior, as it avoids acting on potentially malicious or spoofed messages before a secure context is established. Therefore, the UE's actions in this scenario are in line with 3GPP security requirements. 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, 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) to the UE, and the UE responded with an identity response. Importantly, the identity request from the AMF was sent as a plain (unencrypted) message, and the UE responded before the 5G-AKA procedure was completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard, the UE should only respond to identity requests with sensitive information (such as SUCI or SUPI) in plain NAS messages before security is activated if the request is for SUCI, which is a privacy-preserving identifier designed to be safe for transmission in the clear. If the AMF had requested the SUPI (the permanent identifier), responding in plain text would be a security violation. In this case, since the UE responded with the SUCI, which is specifically designed to protect the subscriber's identity even when sent in the clear, the UE's action aligns with the 3GPP security requirements. Therefore, the UE's behavior in this interaction was secure. Secure
19	19	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11986708641052246 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12012410163879395 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3239710330963135 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was protected with integrity using the 128-5G-IA2 algorithm but specified the use of the null ciphering algorithm (5G-EA0), meaning that subsequent NAS messages would not be encrypted, only integrity protected. The UE responded to this command with a Security Mode Reject message, indicating "Security mode rejected, unspecified." According to the 3GPP 5G security standards (TS 33.501), the use of the null ciphering algorithm (5G-EA0) is only permitted in specific, limited scenarios (such as emergency services or when explicitly allowed by policy), and UEs are generally expected to reject security mode commands that attempt to establish a security context with no encryption in normal operation. The UE's rejection of the security mode command in this context demonstrates adherence to the security requirements of the standard, as it prevents the establishment of an insecure communication channel. Therefore, the UE's action was secure and in line with 3GPP expectations. Secure

20	20	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 2f4b62abf69d8352398c608fb3a89563 AUTN: 062d8ab6b7549000811f4ee8b8da8440 ngKSI_TSC: Native security context ngKSI_KSI: 6 UE provided: Authentication response The packet capture during the test using wireshark is: 1.9198977947235107 UE to AMF SACK (Ack=5, Arwnd=106496) , UplinkNASTransport, Authentication response 1.9201328754425049 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Authentication request 2.120612859725952 UE to AMF UplinkNASTransport, Authentication response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF are engaged in the NAS authentication procedure as part of the 5G-AKA process. The UE first sends an authentication response to the AMF, after which the AMF, instead of proceeding to the next step (such as Security Mode Command), sends another authentication request to the UE. Notably, this subsequent authentication request from the AMF is sent in plain (unencrypted) NAS, which is expected since the 5G-AKA procedure has not yet been completed and security context has not been established. The UE, upon receiving this second authentication request, responds again with an authentication response. According to the 3GPP 5G standard (TS 24.501 and TS 33.501), the UE should only respond to authentication requests prior to the completion of the 5G-AKA procedure, and all NAS messages remain unprotected until security activation. However, the key point here is that the AMF sent a repeated authentication request after already receiving an authentication response, which is not a standard sequence. The UE, by responding again with an authentication response, is technically following protocol, as it has not yet received a Security Mode Command and thus has not established a security context. Therefore, the UE's actions are consistent with the 3GPP standard, as it is correct to respond to authentication requests in plain NAS prior to security activation. There is no evidence of the UE sending protected messages before security context establishment, nor is there evidence of the UE refusing to respond to legitimate authentication requests. Thus, the UE's behavior in this scenario is secure and compliant with the 5G standard. 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: 3030303030300078d431f251560000 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, after the initial NAS procedures, the UE sent an authentication response to the AMF. The AMF, under test control, then sent a subsequent authentication request to the UE, but this request was sent in plain (unencrypted) form and included specific authentication parameters (RAND, AUTN, ABBA, etc.). Upon receiving this authentication request, the UE responded with an "Authentication failure (MAC failure)" message. According to the 3GPP 5G standard, the UE is required to verify the integrity of the authentication request using the Message Authentication Code (MAC) and to reject any authentication request that fails this verification, especially if the message is received in plain text before the 5G-AKA procedure is completed and security context is established. The UE's action to respond with an authentication failure due to MAC failure demonstrates that it correctly detected an invalid or tampered authentication request and refused to proceed with authentication under insecure conditions. This behavior aligns with the security requirements of the 5G standard, as it prevents potential replay or man-in-the-middle attacks before a secure context is established. Therefore, the UE's actions in this interaction were secure. Secure

22	22	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3200 RAND: 303030303030300078b457a1d8550000 AUTN: 313131313131313131310057a1d8550000 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 (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security standards, specifically TS 33.501, the authentication and key agreement (5G-AKA) procedure must be completed before any NAS messages can be securely encrypted and integrity protected. If the AMF sends an authentication request in plain text after the authentication response, this is a deviation from the expected protocol flow, as the authentication procedure should not be repeated or sent in plain after a response has already been provided. The UE correctly identified this abnormal behavior and rejected the authentication attempt, indicating that non-5G authentication is unacceptable. This response is in line with 3GPP security requirements, as the UE must not accept authentication procedures that do not conform to the 5G-AKA protocol or that are not properly protected. By refusing to proceed with an insecure or non-standard authentication process, the UE demonstrated secure behavior as per the 5G standard. Secure

23	23	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11994004249572754 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12018203735351562 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.32151198387145996 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was protected using integrity (128-5G-IA2) but specified the use of the null ciphering algorithm (5G-EA0), meaning no encryption would be applied to subsequent NAS messages. The security header indicated that a new security context was being established. Upon receiving this command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, after authentication, the UE and network must negotiate and agree on both integrity and ciphering algorithms to protect NAS signaling. The use of 5G-EA0 (null ciphering) is only permitted under specific, controlled circumstances (such as emergency services or when explicitly allowed by policy), and generally, the UE is expected to reject the use of null ciphering in normal operation to prevent unencrypted signaling, which could expose sensitive information. The UE's action to reject the Security Mode Command when only integrity protection (without encryption) was offered aligns with the security principles of the 5G standard, as it prevents the establishment of a security context that would leave NAS messages unencrypted. Therefore, the UE's behavior in this scenario was secure and in accordance with 3GPP security requirements. Secure

24	24	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 5781adc4c6cd42baaf6e4fe6cef2e17f AUTN: 67373384aeb990006bc203d2c023b868 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication response The packet capture during the test using wireshark is: 0.11973094940185547 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12026000022888184 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.32166409492492676 UE to AMF UplinkNASTransport, Authentication response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF are engaged in the NAS authentication procedure as part of the 5G-AKA process. The UE first sends an authentication response to the AMF, after which the AMF, instead of progressing to the next step (such as Security Mode Command), sends another authentication request in plain (unencrypted) form. The UE then responds again with an authentication response. According to the 3GPP 5G standard, after the initial authentication exchange, the AMF should not send repeated authentication requests unless the previous authentication failed or was invalid, and all authentication messages prior to the completion of 5G-AKA are sent in plain text as security context is not yet established. However, the critical issue here is that the UE, after having already sent a valid authentication response, accepts and processes a subsequent, unexpected authentication request from the AMF and responds to it. This behavior is not compliant with the 3GPP standard, which expects the UE to reject or ignore repeated or out-of-sequence authentication requests to prevent replay or downgrade attacks. By responding to a repeated authentication request, the UE exposes itself to potential security vulnerabilities, such as replay attacks, and does not adhere to the expected security procedures. Therefore, the UE's action 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 initiated NAS communication and, after completing the initial steps, sent an Authentication Response to the AMF. The AMF, under test control, replied with an Authentication Reject message, which was sent in plain (unencrypted) form because the 5G-AKA procedure had not yet been completed—meaning no NAS security context had been established. Upon receiving the Authentication Reject, the UE did not attempt to continue the registration process or respond with further sensitive information; instead, it immediately sent a Deregistration Request to the AMF, also in plain text, as expected before security activation. According to the 3GPP 5G standard (TS 24.501), the UE is required to abort the registration procedure and deregister itself upon receiving an Authentication Reject, and it is permitted to send the Deregistration Request in plain text if security has not been activated. The UE did not process or respond to the Authentication Reject in any way that would expose sensitive information or violate the protocol. Therefore, the UE's actions were in full compliance with the 5G security requirements, and no security breach occurred as a result of its behavior in this scenario. Secure

26	26	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.15973997116088867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15994787216186523 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.3668229579925537 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to use them for NAS message protection. Following this, the AMF sent a "deregistration request" to the UE, which was integrity protected and ciphered, as indicated by the security header (2). The UE responded with a "deregistration accept" message, completing the deregistration process. According to the 3GPP 5G standard, after the security mode command is accepted and security is activated, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, ciphered. The packet capture confirms that the deregistration request from the AMF was protected, and the UE responded appropriately with a deregistration accept message. Since the UE only sent sensitive messages (such as deregistration accept) after security activation and in response to a protected request, and did not transmit any unprotected NAS messages after security was established, the UE's actions align with the security requirements of the 5G standard. Therefore, the UE's behavior in this interaction was secure. Secure
27	27	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.1597728729248047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16001200675964355 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.36782288551330566 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (integrity protection and ciphering) was established. Subsequently, the AMF sent a "deregistration request" message to the UE, which was protected with both integrity and ciphering, as indicated by the security header (2). The UE responded with a "deregistration accept" message, also protected, thereby completing the deregistration process. According to the 3GPP 5G standard, after the 5G-AKA procedure and the establishment of NAS security, all subsequent NAS messages, including deregistration, must be integrity protected and ciphered to ensure confidentiality and authenticity. The packet capture confirms that the UE only sent protected messages after security was established and responded appropriately to the AMF's deregistration request. There is no indication that the UE accepted or processed any unprotected or insecure messages after the security context was set up. Therefore, the UE's actions were in line with 3GPP security requirements, maintaining the integrity and confidentiality of NAS signaling. Secure

28	28	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.16000795364379883 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602778434753418 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36232805252075195 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to proceed with protected NAS communication. However, the AMF then sent another "security mode command" message, this time protected, instructing the UE to re-enter security mode negotiation. Notably, the ciphering algorithm selected was 128-5G-EA2, but the integrity algorithm was set to 5G-IA0 (null), meaning no integrity protection would be applied to subsequent NAS messages. Upon receiving this command, the UE responded with a "security mode reject" message, refusing to proceed with the new security mode and indicating an unspecified reason for rejection. According to the 3GPP 5G standard, integrity protection is mandatory for NAS signaling to prevent tampering and replay attacks; the use of a null integrity algorithm (5G-IA0) is not permitted for normal operation and should be rejected by compliant UEs. The UE's action to reject the security mode command that proposed a null integrity algorithm aligns with the security requirements of the standard, as it prevents the establishment of a vulnerable security context. Therefore, the UE's behavior in this scenario was secure and in accordance with 3GPP specifications. Secure

29	29	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.15992307662963867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16016101837158203 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36194396018981934 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to proceed with protected NAS communication. However, the AMF then sent another "security mode command" message, this time protected and specifying the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, which effectively means no encryption or integrity protection would be applied to subsequent NAS messages. Upon receiving this, the UE responded with a "security mode reject" message, refusing to accept the proposed security configuration. According to the 3GPP 5G standard (TS 24.501), the use of null algorithms is only permitted under very specific circumstances (such as emergency services or when explicitly allowed by the UE's security policy), and UEs are expected to reject security mode commands that attempt to downgrade security to null algorithms outside of these cases. The UE's action to reject the security mode command with null algorithms demonstrates adherence to the 5G security requirements and protects against potential security downgrades or attacks. Therefore, the UE's behavior in this scenario was secure and compliant with the 3GPP standard. Secure

30	30	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected (1) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.16007494926452637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037607192993164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.364534854888916 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating its acceptance of the negotiated security algorithms (5G-EA7 for ciphering and 128-5G-IA2 for integrity protection). However, the AMF then sent a "security mode command" message to the UE, which is unusual because, according to the 3GPP 5G standard, the security mode command should be sent by the AMF **before** the UE sends the security mode complete. The correct sequence is: after 5G-AKA, the AMF sends a security mode command to the UE, the UE responds with security mode complete, and only then are subsequent NAS messages protected using the agreed algorithms. In this test, the UE sent a security mode complete **before** receiving the security mode command, and then, after receiving the security mode command, it again sent a security mode complete. This indicates that the UE accepted and responded to a security mode command **after** it had already indicated completion of the security mode procedure, which is not compliant with the 3GPP standard and could potentially expose the UE to replay or downgrade attacks if the security context is not properly managed. The UE should only send a security mode complete **in direct response** to a security mode command, and not before. Therefore, the action taken by the UE was **insecure** as it did not follow the correct 5G security procedure and could compromise the integrity of the security context. 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 (5G-EA4 for ciphering and 5G-IA0, which is null, for integrity). The AMF then sent a "security mode command" message, which was protected, and the UE subsequently sent a "deregistration request (UE originating)" message. According to the 3GPP 5G standard, after 5G-AKA and the security mode command/complete exchange, all subsequent NAS messages should be both ciphered and integrity protected, except in specific cases (e.g., emergency services or when null algorithms are negotiated). In this test, the integrity algorithm selected was 5G-IA0 (null), meaning that while messages could be encrypted (ciphered with 5G-EA4), they were not integrity protected. The use of a null integrity algorithm is generally discouraged in commercial deployments because it leaves the communication vulnerable to modification attacks, even if the content is encrypted. The UE's acceptance and use of 5G-IA0 for integrity, and its subsequent sending of a deregistration request under these conditions, is not considered secure by 3GPP standards, as it does not provide the required integrity protection for NAS signaling. Therefore, the UE's actions in this scenario are insecure. Insecure

32	32	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.1595141887664795 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15984320640563965 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to begin protected NAS communication. However, the AMF then sent another "security mode command" message, this time with the security header set to "integrity protected and ciphered," using the agreed-upon cipher (5G-EA4) and integrity (128-5G-IA3) algorithms. The UE did not respond to this subsequent security mode command. According to the 3GPP 5G standard, once the security mode complete message is sent and security is activated, the UE should not expect another security mode command in the same registration procedure; receiving such a message could indicate a protocol anomaly or a potential security attack (such as a replay or downgrade attempt). The UE's lack of response to this unexpected, protected security mode command demonstrates correct and secure behavior, as it avoids engaging in potentially insecure or non-standard protocol flows. This action aligns with 3GPP security guidelines, which require the UE to ignore or reject unexpected or out-of-sequence security messages to prevent exploitation. Therefore, the UE's behavior in this scenario was secure. Secure
33	33	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 6 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.16021108627319336 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 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) was established. The AMF then sent a protected (i.e., encrypted and integrity-protected) GMM status message with a 5GMM cause value of 6, which corresponds to "Illegal ME" (Mobile Equipment). Upon receiving this status message, the UE responded by sending a deregistration request (UE originating) to the AMF. According to the 3GPP 5G standard (TS 24.501), after security mode is complete, all subsequent NAS messages must be protected, and the UE must react appropriately to status messages, especially those indicating severe errors such as "Illegal ME." The UE's action to deregister itself upon receiving an "Illegal ME" cause is compliant with the standard, as it is expected to cease network access attempts when notified of such a condition. The packet capture confirms that the messages were exchanged after security was established, and the UE did not send any unprotected or unexpected messages. Therefore, the UE's behavior was secure and in line with 3GPP requirements. Secure

34	34	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.15963101387023926 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15987801551818848 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.360584020614624 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (integrity protection and ciphering) was established. Subsequently, the AMF sent a "deregistration request" message to the UE, which was protected with both integrity and ciphering, as indicated by the security header (2). The UE responded with a "deregistration accept" message, also protected, thereby completing the deregistration process. According to the 3GPP 5G standard, once NAS security is established, all subsequent NAS messages, including deregistration procedures, must be integrity protected and ciphered to prevent interception or tampering. The packet capture confirms that the UE only sent protected messages after security activation, and responded appropriately to a valid, protected deregistration request. Therefore, the UE's actions adhered to the security requirements of the 5G standard, ensuring that sensitive signaling was not exposed in cleartext and that the UE did not process unprotected or suspicious messages. Based on this analysis, the UE's behavior was secure and compliant with 3GPP specifications. Secure
35	35	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.15990018844604492 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16015410423278809 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was completed, establishing the necessary security context for subsequent NAS message protection. The UE then 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 protecting NAS messages. Following this, the AMF sent a "service accept" message to the UE, which was correctly protected (i.e., integrity protected and/or ciphered) as per the 3GPP 5G NAS security requirements. However, after receiving the protected "service accept" message, the UE did not respond further. According to the 3GPP 5G standard, once the security context is established and NAS security is activated, the UE must only accept and process protected NAS messages; unprotected messages should be ignored or rejected. In this case, the UE received a protected message and, by not responding, did not process or act upon any unprotected or suspicious messages. This behavior aligns with the security requirements, as the UE did not compromise the security context or accept unprotected messages after security activation. Therefore, the UE's actions were in accordance with the 3GPP 5G security standards and did not expose any vulnerabilities in this interaction. Secure

36	36	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5051651000976562 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5054340362548828 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7091829776763916 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context was established and that subsequent NAS messages would be protected. The AMF, under test control, then sent a "Deregistration Request (UE terminated)" message to the UE, which was integrity protected and ciphered, as indicated by the security header (2). The UE responded appropriately with a "Deregistration Accept (UE terminated)" message, also protected as per the established security context. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages between the UE and AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The UE's actions—accepting and responding to a protected deregistration request only after security was established—demonstrate compliance with these requirements. There is no indication that the UE accepted or responded to any unprotected or insecure messages after the security context was set up. Therefore, the UE's behavior in this interaction aligns with the security expectations of the 5G standard and does not expose any vulnerabilities in the tested scenario. 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 procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration process was finalized. The AMF then responded with a "Service Accept" message, which was sent as a protected (i.e., integrity protected and/or ciphered) NAS message, confirming that security context was established and NAS security was active. Subsequently, the UE sent a "Deregistration Request (UE originating)" message to the AMF. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be protected using the established security context. The packet capture shows that the "Service Accept" message from the AMF was protected, which is correct. The critical point is whether the UE's "Deregistration Request" was also sent as a protected message. While the packet capture summary does not explicitly state the protection status of the deregistration request, the fact that the 5G-AKA was completed and the AMF was sending protected messages strongly suggests that the UE should also be sending its messages in a protected manner, as required by the standard. If the deregistration request was indeed protected, the UE's actions would be secure and compliant with 3GPP requirements. However, if it was sent unprotected, that would be a security flaw. Based on the information provided and the sequence of events, it appears the UE followed the expected secure behavior after 5G-AKA completion. Secure

38	38	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.5716309547424316 UE to AMF UplinkNASTransport, Registration complete 0.5718338489532471 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS procedures were finished. Subsequently, the AMF sent a "Security Mode Command" message to the UE, which was integrity protected using the new security context established during 5G-AKA, with the ciphering algorithm set to 5G-EA0 (null, meaning no encryption) and the integrity algorithm set to 128-5G-IA2. The security header indicated that the message was integrity protected with a new security context. According to the 3GPP 5G standard, after 5G-AKA, the network should initiate NAS security mode control to establish ciphering and integrity protection for subsequent NAS messages. However, the use of 5G-EA0 (null ciphering) means that messages are not encrypted, only integrity protected. The UE, upon receiving a Security Mode Command with null ciphering, is expected to respond only if it supports this configuration and if it is allowed by the operator policy and security requirements. In this test, the UE did not respond to the Security Mode Command, which suggests that it refused to proceed with a null ciphering algorithm, thereby preventing unencrypted communication. This behavior aligns with security best practices and the 3GPP standard, which allows the UE to reject insecure configurations. Therefore, the UE's action was secure, as it did not accept a security context that would have left its NAS messages unencrypted. Secure
39	39	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.2683730125427246 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2686209678649902 AMF to UE SACK (Ack=12, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.476357936859131 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context was established. Following this, the AMF sent a "Configuration Update Command" to the UE, which was observed in the packet capture as being integrity protected and ciphered, as indicated by the security header (value 2). The UE then responded with a "Configuration Update Complete" message. According to the 3GPP 5G standard, after the 5G-AKA procedure, all subsequent NAS messages exchanged between the UE and the AMF must be both integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The packet capture confirms that the downlink message from the AMF was indeed protected, and the UE responded appropriately within the secured NAS context. Since the UE only sent messages after the security context was established and responded to protected messages as required by the standard, the actions taken by the UE align with 3GPP security requirements for NAS communication. Therefore, based on the observed behavior and adherence to the standard, the UE's actions were secure. Secure

40	40	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.427475929260254 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.427738904953003 AMF to UE SACK (Ack=12, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.6314868927001953 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "registration complete" message to the AMF, indicating that the initial NAS security context was established. Following this, the AMF sent a "configuration update command" to the UE, which was observed in the packet capture as being integrity protected and ciphered, as indicated by the security header (value 2). The UE then responded with a "configuration update complete" message. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be both integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The packet capture confirms that the downlink message from the AMF was protected, and the UE responded appropriately within the secured NAS context. Since the UE only sent messages after the security context was established and responded to protected messages as required by the standard, the actions taken by the UE align with 3GPP security requirements. Therefore, the UE's communication in this scenario was secure. Secure

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) and specified the use of 128-5G-EA2 for ciphering and 128-5G-IA2 for integrity protection, as per 3GPP standards. However, the UE did not respond to this Security Mode Command, and instead, shortly after, initiated a new "InitialUEMessage" with a "Service Request," which was subsequently rejected by the AMF. According to 3GPP TS 24.501, after receiving a Security Mode Command, the UE is required to process the command, establish the new security context, and respond with a Security Mode Complete message before sending any further NAS messages. The UE’s failure to respond to the Security Mode Command and its attempt to send a new Service Request without first establishing the agreed security context is a deviation from the standard and exposes the communication to potential security risks, such as replay or man-in-the-middle attacks. This behavior indicates that the UE did not properly enforce the required security procedures after authentication, making its actions non-compliant with 3GPP security requirements. Insecure
42	42	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.513239860534668 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5140058994293213 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5144908428192139 AMF to UE DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an UplinkNASTransport message to the AMF, which is expected behavior as NAS security should be active at this stage. The AMF, under test control, responded with a protected Deregistration Accept message, indicating the termination of the UE's registration. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. The packet capture shows that the AMF sent the Deregistration Accept message as protected, but the UE did not respond to this message. Per 3GPP specifications, upon receiving a protected Deregistration Accept message, the UE is not required to send any further response; the deregistration procedure is considered complete from the UE's perspective. Therefore, the UE's lack of response is compliant with the standard and does not indicate a security flaw. The UE maintained the expected security posture by not responding unnecessarily and by only communicating after security activation. Secure

43	43	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5069518089294434 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5071558952331543 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5073068141937256 AMF to UE DownlinkNASTransport 0.7109389305114746 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending a Configuration Update Command. The packet capture shows that the Configuration Update Command from the AMF was sent as a protected message, with the security header indicating both integrity protection and ciphering, which is in line with 3GPP 5G security requirements that mandate NAS messages be protected after security establishment. Subsequently, the UE responded with a Deregistration Request (UE originating), which was also sent as an Uplink NAS Transport message. Since the 5G-AKA procedure was completed prior to these exchanges, the security context was established, ensuring that subsequent NAS messages—including the deregistration request from the UE—were encrypted and integrity protected. This behavior aligns with the 3GPP 5G standard, which requires that after security mode is activated, all NAS signaling messages between the UE and AMF must be protected. There is no indication that the UE sent any unprotected or insecure messages after the security context was established. Therefore, the UE's actions in this interaction were secure and compliant with the 5G standard. Secure
44	44	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 6.589772939682007 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.5903379917144775 AMF to UE SACK (Ack=18, Arwnd=106401) , DownlinkNASTransport, Configuration update command 6.590748071670532 AMF to UE DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 6.793751955032349 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE proceeded to send uplink NAS messages, including a UL NAS transport, to the AMF. The AMF, under test control, then sent a deregistration request to the UE, which was protected with both integrity and ciphering as indicated by the security header (2). The UE responded appropriately with a deregistration accept message, indicating that it processed the request and terminated its registration as instructed. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be protected using integrity and ciphering to ensure confidentiality and authenticity. The packet capture confirms that the deregistration request from the AMF was indeed protected, and the UE responded only after receiving this protected message. There is no indication that the UE accepted or acted upon any unprotected or suspicious messages, nor did it send any sensitive information in the clear. Therefore, the UE's actions align with the security requirements of the 5G standard, as it only responded to a properly protected deregistration request after secure authentication was established. Secure

45	45	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5155510902404785 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5157649517059326 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5159080028533936 AMF to UE DownlinkNASTransport, Configuration update command 0.7195420265197754 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, indicating that the security context was already established. Subsequently, the AMF sent a Configuration Update Command to the UE, which was observed in the packet capture as being integrity protected and ciphered, as indicated by the security header (value 2). The UE then responded with a Configuration Update Complete message, also sent as an Uplink NAS Transport, which, given the established security context, would also be protected. According to the 3GPP 5G standard, after the 5G-AKA procedure, 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 packet capture and message flow confirm that the UE only sent sensitive messages after the security context was established and responded appropriately to protected messages from the AMF. Therefore, the UE's actions adhered to the security requirements of the 5G standard, ensuring that all NAS communications post-authentication were properly protected. 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. The packet capture shows that the Configuration Update Command from the AMF was sent as a protected message, specifically with a security header indicating both integrity protection and ciphering, which aligns with 3GPP 5G security requirements for NAS signaling after authentication. The UE then responded with a Configuration Update Complete message, also sent as an Uplink NAS Transport, indicating that it processed the command and maintained the secure communication context established during 5G-AKA. 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 to ensure confidentiality and authenticity. The actions taken by the UE—accepting and responding to a protected Configuration Update Command only after 5G-AKA completion—demonstrate adherence to these security requirements. Therefore, based on the observed behavior and the 3GPP standard, the UE’s actions were secure. Secure

47	47	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.4281399250030518 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4283440113067627 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.428462028503418 AMF to UE DownlinkNASTransport, Configuration update command 2.6321370601654053 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, indicating that the security context was 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 transmitted with a security header indicating both integrity protection and ciphering (security header type 2). The UE responded with a Configuration Update Complete message, also sent as an Uplink NAS Transport, which would be expected to be protected under the established NAS security context. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed, all subsequent NAS messages between the UE and AMF must be integrity protected and, where required, ciphered. The packet capture and test summary confirm that the Configuration Update Command from the AMF was protected, and the UE responded appropriately, indicating that it adhered to the security requirements. Therefore, based on the observed behavior and compliance with the 3GPP standard, the UE's actions were secure. Secure

48	48	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3200 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 2.4352028369903564 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4353890419006348 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.435595989227295 AMF to UE DownlinkNASTransport, Security mode command 2.6392359733581543 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, indicating that it was ready for further NAS communication. The AMF, under test control, responded with a Security Mode Command message, which was properly protected (integrity protected with a new security context) and specified the use of 5G-EA4 for ciphering and 128-5G-IA2 for integrity protection, along with an ABBA value of 3200. Upon receiving this Security Mode Command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, after 5G-AKA, the UE is expected to accept a valid Security Mode Command if the parameters (algorithms, ABBA, etc.) are supported and the message is properly protected. A Security Mode Reject is only expected if the UE detects an issue such as unsupported algorithms, invalid ABBA, or a problem with the security context. Since the Security Mode Command was sent with standard algorithms and proper protection, and the UE rejected it without specifying a clear reason, this behavior could indicate a security-conscious implementation (e.g., rejecting unexpected or suspicious parameters) or a misconfiguration/bug in the UE. However, since the rejection was "unspecified" and the message was properly protected, the UE's action aligns with a cautious security posture, refusing to proceed with potentially unsafe or unrecognized security parameters, which is preferable to accepting a potentially insecure context. Therefore, the UE's action can be considered secure, as it did not accept a security context it was not fully confident in. Secure

49	49	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 17.321523904800415 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.322353839874268 AMF to UE SACK (Ack=24, Arwnd=106496) , DownlinkNASTransport, Security mode command 17.532354831695557 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was integrity protected and indicated the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm, with the security header set to "integrity protected with new security context." Upon receiving this, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, after authentication, the AMF should select appropriate ciphering and integrity algorithms based on the UE's capabilities and network policy. The use of the null ciphering algorithm (5G-EA0) means that user data would not be encrypted, which is generally only allowed in specific, controlled scenarios (such as emergency services or when explicitly permitted by policy). If the UE does not support or is not configured to accept null encryption in normal operation, it is expected to reject such a security configuration to prevent unprotected data transmission. Therefore, the UE's action to reject the Security Mode Command when presented with null encryption is in line with secure behavior as defined by the 3GPP standard, as it prevents the establishment of an insecure communication channel. Secure
50	50	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 24.788990020751953 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 24.789222955703735 AMF to UE SACK (Ack=27, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is a standard step to resume or establish a session. In response, the AMF sent a Deregistration Accept message, encapsulated within a DownlinkNASTransport and marked as "Protected," indicating that it was integrity protected and/or encrypted as per 3GPP security requirements post-authentication. The UE, upon receiving this protected Deregistration Accept message, did not respond further. According to the 3GPP 5G security standards, after 5G-AKA, all NAS messages must be integrity protected and, where required, encrypted. The UE's lack of response to a properly protected Deregistration Accept message is a secure behavior, as it indicates that the UE did not process or act upon any unprotected or suspicious messages, and it did not continue communication after being deregistered. This aligns with the expected secure operation, as the UE should cease NAS communication upon receiving a valid, protected deregistration message. Therefore, the UE's actions in this scenario were in accordance with 3GPP security standards. Secure

51	51	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 25.642455101013184 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 25.642899990081787 AMF to UE SACK (Ack=24, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Message type not compatible with the protocol state) 25.85011601448059 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE initiated a service request to the AMF, indicating that a secure NAS security context was already established. The AMF, under test control, responded with a deregistration request (UE terminated), which was sent as a protected NAS message—specifically, it was both integrity protected and ciphered, as indicated by the security header (2). The UE, upon receiving this protected deregistration request, responded with a deregistration accept message, also sent as a protected NAS message. According to the 3GPP 5G standard, once the NAS security context is established, all subsequent NAS messages, including deregistration procedures, must be integrity protected and ciphered to ensure confidentiality and authenticity. The UE's actions—accepting and responding to a properly protected deregistration request—are in line with the expected secure behavior as per the standard. The fact that the deregistration request was sent in a protected manner and the UE responded accordingly demonstrates that the UE adhered to the security requirements, even though the deregistration request was unexpected in the protocol state. Therefore, the UE's actions were secure and compliant with 3GPP 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 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 responded with a configuration update command, sent as a downlink NAS message that was both integrity protected and ciphered, indicating that the NAS security context was active and the message was encrypted and authenticated as per 3GPP requirements. Upon receiving this protected message, the UE responded with a deregistration request (UE originating), which was sent via an UplinkNASTransport message. Since the 5G-AKA procedure was completed prior to these exchanges, all subsequent NAS messages, including the deregistration request, would be expected to be protected by the established security context. The UE's action to send a deregistration request after receiving a protected configuration update command is within the expected behavior, as the UE is allowed to deregister at any time, and there is no indication that the UE sent any unprotected or out-of-specification messages. The use of integrity protection and ciphering for the downlink message further confirms that the security procedures were followed. Therefore, based on the 3GPP 5G security standards, the UE's actions in this interaction were secure and compliant with the expected protocol behavior. Secure

53	53	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 17.000593185424805 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.001089096069336 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal UE) 17.204612970352173 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE initiated a service request to the AMF, indicating that the NAS security context was established and subsequent NAS messages would be protected. In response, the AMF sent a deregistration request (UE terminated), which was integrity protected and ciphered, as indicated by the security header (2). The UE then responded with a deregistration accept message, also protected, completing the deregistration process. According to 3GPP standards (TS 24.501), once the NAS security context is established, the UE must only accept and respond to protected NAS messages, and must not process unprotected messages that require security. In this interaction, the UE correctly processed a protected deregistration request and responded appropriately with a protected deregistration accept, demonstrating adherence to the security requirements of the 5G standard. There is no indication that the UE accepted or responded to any unprotected or improperly protected messages, nor did it behave in a way that would compromise the security context. Therefore, based on the observed actions and compliance with 3GPP security procedures, the UE's behavior in this scenario was secure. Secure
54	54	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 100 UE provided: No response The packet capture during the test using wireshark is: 1.321023941040039 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.3216829299926758 AMF to UE DownlinkNASTransport, 5GMM status (Conditional IE error) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a Service Request message to the AMF, which is a standard step to resume or establish a user session. The AMF then responded with a GMM Status message indicating a "Conditional IE error" (5GMM Cause: 100), and this message was sent as a protected (encrypted and integrity-protected) NAS message, as expected after 5G-AKA completion. The UE, upon receiving this protected GMM Status message, did not respond further. According to the 3GPP 5G standards (TS 24.501), when a UE receives a GMM Status message with an unrecognized or irrelevant cause value, or if the message indicates an error that the UE cannot recover from, it is permissible for the UE to silently discard the message and not respond, especially if the message is protected and the integrity is verified. This behavior prevents unnecessary signaling and potential security vulnerabilities that could arise from responding to malformed or unexpected messages. Therefore, the UE's action of not responding to the protected GMM Status message with cause 100 is consistent with secure and standard-compliant behavior as outlined by 3GPP. Secure

55	55	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003898143768310547 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the initial NAS messages exchanged before authentication (including Registration Request and Authentication Reject) are permitted to be sent in plain text, as encryption and integrity protection are only established after successful completion of the 5G-AKA procedure. The UE, upon receiving the Authentication Reject message, did not respond further, which is the expected and secure behavior as per the standard; the UE should not proceed with registration or attempt to establish a secure context after receiving such a rejection. Therefore, the UE's actions—sending the initial request, receiving a plain Authentication Reject, and not responding further—are in line with 3GPP security requirements and do not expose the UE to additional risk in this context. Secure
56	56	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00040602684020996094 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are permitted to be sent in plain text, as encryption and integrity protection are not yet available. The UE, upon receiving an Authentication Reject message in plain text before security activation, is expected to not respond further, as per the standard, to avoid unnecessary exposure or further communication without security. In this test, the UE did not respond to the plain Authentication Reject, which aligns with the expected secure behavior defined by 3GPP: the UE should not proceed with any further NAS communication after receiving an Authentication Reject, especially before security is established. Therefore, the UE's action was secure and compliant with the 5G standard. 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, 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 to enable encryption and integrity protection. The UE, upon receiving the plain Authentication Reject, did not respond further, which is compliant with the standard: the UE is expected to abort the registration procedure and not proceed with any further NAS signaling in this case. This behavior prevents the UE from exposing itself to further potential attacks or information leakage. Therefore, the UE's action—ceasing communication after receiving a plain Authentication Reject before security context establishment—aligns with 3GPP security requirements and is considered secure. Secure
58	58	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003209114074707031 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should treat any plain (unencrypted and unauthenticated) NAS messages received before the completion of 5G-AKA with caution, as these messages could be spoofed by an attacker. The correct and secure behavior for the UE, as outlined in the standard, is to ignore or silently discard such unauthenticated messages, especially critical ones like Authentication Reject, until a security context is established. In this test, the UE did not respond to the plain Authentication Reject message, which aligns with the 3GPP security recommendations and helps prevent downgrade or denial-of-service attacks that could be triggered by unauthenticated messages. Therefore, the UE's action in this scenario was secure. Secure

59	59	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0002620220184326172 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should treat any plain (unencrypted and unauthenticated) NAS messages received before the completion of 5G-AKA with caution, as these messages could be spoofed by an attacker. The standard mandates that the UE must not take any further action or respond to such messages, to prevent security breaches such as false base station attacks (e.g., IMSI catchers). In this test, the UE did not respond to the plain Authentication Reject message, which aligns with the 3GPP security requirements and demonstrates correct, secure behavior. The UE's lack of response ensures that it does not act on potentially malicious or unauthenticated messages, thereby protecting itself and the network from possible attacks. Secure
60	60	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003459453582763672 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should only accept certain NAS messages in plain text prior to the completion of authentication, and it must be cautious in handling Authentication Reject messages received in the clear. The standard mandates that if the UE receives an Authentication Reject message before security context is established (i.e., before 5G-AKA is completed), it should treat this as a potential security threat, as such messages could be sent by an attacker to cause a denial of service or to impersonate the network. The correct and secure behavior for the UE, as per the standard, is to ignore the Authentication Reject message received in plain text before authentication is completed and not to respond to it. In this test, the UE did not respond to the plain Authentication Reject message, which aligns with the 3GPP security requirements and demonstrates secure behavior in the face of a potential attack. 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 for NAS message encryption and integrity protection was not yet established. According to the 3GPP 5G standard, specifically TS 24.501, it is expected that the initial NAS messages, including registration request and registration reject, are exchanged in plain text before the security context is set up. The UE, upon receiving a plain registration reject before security activation, is expected to accept and process it, as this is compliant with the standard. The UE did not respond further, which is also in line with expected behavior, as a registration reject is a terminal message for that procedure. Therefore, the UE's actions were secure and compliant with the 3GPP standard, as it did not accept any insecure messages after security activation and properly handled the plain registration reject before security was established. Secure
62	62	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 17.596633911132812 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.597079038619995 AMF to UE SACK (Ack=14, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a service request to the AMF, which is a standard procedure for requesting network services. The AMF, under test control, responded with a protected (i.e., integrity protected and/or ciphered) "deregistration accept" message, which is typically sent in response to a deregistration request from the UE, not as a response to a service request. According to the 3GPP 5G standards, the UE should only process a "deregistration accept" message if it has previously initiated a deregistration procedure; otherwise, it should ignore such unsolicited messages, especially if they are unexpected or out of sequence. In this test, the UE did not respond to the unsolicited "deregistration accept" message, which indicates that it correctly ignored an out-of-context message, thereby preventing potential misuse or session hijacking. This behavior aligns with the security requirements of the 5G standard, as the UE did not accept or act upon an unexpected network command, maintaining the integrity of its state machine and protecting itself from possible attacks. Secure

63	63	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0203 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.10306811332702637 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.10332202911376953 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3094031810760498 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an Authentication Response to the AMF, which is the expected behavior. The AMF then sent a Security Mode Command, which was protected using the negotiated ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms, and the security header indicated that the message was integrity protected with a new security context, as per 3GPP standards. Following this, the UE sent a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G security architecture, after the Security Mode Command is successfully received and processed, the UE should use the established security context to protect subsequent NAS messages. The packet capture shows that the Security Mode Command was protected, and the UE did not send any unprotected NAS messages after security activation. The Deregistration Request was sent after security context establishment, which means it should have been protected as per the standard. There is no indication in the summary that the Deregistration Request was sent unprotected or that the UE failed to follow the security procedures. Therefore, based on the information provided and the sequence of actions, the UE's behavior aligns with the 3GPP 5G security requirements, and the communication can be considered secure. Secure
64	64	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 17.12326717376709 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 17.123653173446655 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a standard step for requesting access to network services. The AMF responded with a service accept message, which, according to the packet capture, was sent as a protected (i.e., integrity protected and/or ciphered) NAS message. However, the UE did not provide any response to this protected downlink message from the AMF. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered to ensure confidentiality and authenticity. The UE is expected to process protected messages and respond appropriately, such as by acknowledging the service accept or proceeding with the next steps in the session establishment. The lack of response from the UE to a properly protected service accept message indicates a failure to comply with the expected secure behavior as defined by the standard. This could expose the UE to potential security risks, such as denial of service or session hijacking, if it is unable to handle protected messages correctly. Therefore, based on the observed behavior, the UE's action in this scenario is considered insecure. Insecure

65	65	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.15958499908447266 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16092395782470703 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36401796340942383 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to proceed with protected NAS communication. However, the AMF then sent another "security mode command" message, this time protected with the newly established security context. Upon receiving this unexpected and redundant security mode command, the UE responded with a "security mode reject" message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, once the security mode procedure is completed and acknowledged by the UE, the AMF should not initiate another security mode command unless there is a valid reason, such as a change in security context or a handover. The UE's action to reject the second, unnecessary security mode command is consistent with the standard's security principles, as accepting repeated or unexpected security mode commands could expose the UE to downgrade or replay attacks. By rejecting the redundant command, the UE demonstrated secure behavior by adhering to the expected protocol flow and protecting itself from potential security risks. Secure

66	66	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0322 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 2.5863499641418457 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.5868079662323 AMF to UE SACK (Ack=9, Arwnd=106361) , DownlinkNASTransport, Configuration update command 2.5871849060058594 AMF to UE DownlinkNASTransport, Security mode command 2.7903499603271484 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, indicating it was ready for further NAS communication. The AMF, under test control, responded with a Security Mode Command message that was protected using the negotiated security algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity protection) and included a new security context, as indicated by the security header. The UE, upon receiving this Security Mode Command, responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, after 5G-AKA, the UE is expected to accept a valid Security Mode Command that is properly protected and uses the correct security context and algorithms. A Security Mode Reject is only expected if the UE detects an error, such as an unsupported algorithm, an invalid security context, or a malformed message. In this case, since the Security Mode Command was sent with the correct protection and context, and the algorithms were standard, the UE's rejection without a specific cause ("unspecified") suggests that it did not follow the expected secure behavior as per 3GPP standards. A secure UE should only reject the Security Mode Command for a well-defined, standards-based reason and should indicate the specific cause. Therefore, the UE's action in this scenario is considered insecure, as it does not align with the 3GPP requirements for secure and standards-compliant communication following successful authentication and security context establishment. Insecure

67	67	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.8137481212615967 UE to AMF UplinkNASTransport, Service request 0.814223051071167 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Unknown) 1.0217480659484863 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Service Request to the AMF, which is a standard procedure to initiate communication or resume a session. The AMF, under test control, responded with a protected (encrypted and integrity-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. Upon receiving this, the UE replied with its own GMM Status message, echoing the same cause. According to the 3GPP 5G NAS protocol, the UE is expected to respond with a Status message when it receives a message that is not compatible with its current protocol state, especially if the message is protected and the security context is active (as 5G-AKA was completed). The UE's action demonstrates correct protocol behavior: it did not process the unexpected or invalid message, but instead reported the protocol error back to the AMF using a protected Status message. This ensures that the UE does not act on potentially malicious or malformed messages, maintaining the integrity and security of the NAS communication as per 3GPP standards. Therefore, the UE's response was secure and compliant with the 5G standard. Secure
68	68	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.7269129753112793 UE to AMF UplinkNASTransport, Service request 0.7272160053253174 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.9349148273468018 UE to AMF UplinkNASTransport, Configuration update complete, UplinkNASTransport, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 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 responded with a Configuration Update Command, which was sent as a protected message with integrity protection enabled, as indicated by the security header. The UE then replied with a Configuration Update Complete message, acknowledging the configuration update, and subsequently sent a Registration Request. According to the 3GPP 5G security standards, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected, and, where required, encrypted to ensure confidentiality and authenticity. The packet capture confirms that the Configuration Update Command from the AMF was integrity protected, and the UE responded appropriately with the expected acknowledgment. There is no indication that the UE sent any unprotected or unencrypted messages after the security context was established, nor did it accept or process any unprotected messages from the AMF. Therefore, based on the observed behavior and adherence to the 3GPP security requirements, the UE's actions in this interaction were secure. Secure

69	69	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3100 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11985111236572266 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12013506889343262 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3252840042114258 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was integrity protected and indicated the use of the 5G-EA0 (null) ciphering algorithm and 128-5G-IA2 for integrity protection. The security header specified that the message was integrity protected with a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G 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, leaving user and signaling data unprotected. The 3GPP standard (TS 33.501) allows the UE to reject a security mode command if it deems the proposed security algorithms insufficient, especially if only null encryption is offered, as this could expose the UE to security risks. The UE's decision to reject the security mode command in this context demonstrates adherence to security best practices by refusing to operate without encryption, thereby protecting user data and signaling integrity. Therefore, the UE's action was secure and compliant with 3GPP security requirements. Secure

70	70	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.547684907913208 UE to AMF UplinkNASTransport, Registration complete 0.5478739738464355 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security procedures had been completed. Subsequently, the AMF sent a "Security Mode Command" message to the UE, which was protected (integrity protected and ciphered with a new security context), specifying the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm. The UE, however, did not respond to this message. According to the 3GPP 5G standard, after the 5G-AKA procedure, the UE and AMF should establish NAS security, and the UE is expected to respond to a valid Security Mode Command with a Security Mode Complete message, provided the command is valid and the security context is correct. In this case, the AMF requested the use of the null ciphering algorithm (5G-EA0), which means that subsequent NAS messages would not be encrypted, only integrity protected. The 3GPP standard allows the use of 5G-EA0 in certain scenarios (e.g., for emergency services or if the UE does not support other algorithms), but in normal operation, the use of a null cipher is discouraged as it exposes NAS messages to potential eavesdropping. The UE's refusal to respond to the Security Mode Command that specified 5G-EA0 can be interpreted as a security-conscious action, as it avoids downgrading the security of the NAS communication. Therefore, the UE's action aligns with best security practices and the intent of the 3GPP standard to avoid the use of null encryption unless absolutely necessary. Secure

71	71	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0332 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 4.62968111038208 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 4.630121946334839 AMF to UE SACK (Ack=10, Arwnd=106361) , DownlinkNASTransport, Configuration update command 4.6305460929870605 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the UE continues with NAS signaling. The AMF then responded with a Security Mode Command, which was protected using the selected ciphering algorithm (128-5G-EA3) and a null integrity algorithm (5G-IA0), and the security header indicated that the message was both integrity protected and ciphered. According to the 3GPP 5G standard, after 5G-AKA, the Security Mode Command is used to establish NAS security, and the UE is expected to respond with a Security Mode Complete message to confirm acceptance of the security context. However, in this test, the UE did not respond to the Security Mode Command. This lack of response is not compliant with the 3GPP standard, as the UE should either accept the security context and respond, or reject it with an appropriate message. The absence of any response could indicate a failure to process the protected message, a misconfiguration, or a security issue in the UE's NAS stack. Since the UE did not follow the expected secure protocol flow by failing to respond, its action is considered insecure according to the 3GPP standard. Insecure

72	72	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3300 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 6.590965032577515 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.591464042663574 AMF to UE SACK (Ack=25, Arwnd=106401) , DownlinkNASTransport, Configuration update command 6.5918920040130615 AMF to UE DownlinkNASTransport, Security mode command 6.7950029373168945 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, indicating it was ready for further NAS communication. The AMF then sent a Security Mode Command message, which was protected and specified the use of ciphering algorithm 5G-EA5 and integrity algorithm 128-5G-IA2, with the security header indicating "integrity protected with new security context." The UE responded with a Security Mode Reject message, citing "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, after 5G-AKA, the UE is expected to accept a Security Mode Command if the parameters (algorithms, ABBA, etc.) are supported and valid. A Security Mode Reject is only expected if the UE detects an issue such as unsupported algorithms, invalid parameters, or a security concern (e.g., a mismatch in the negotiated security context or an attempt to downgrade security). Since the Security Mode Command was protected and followed the expected sequence, the UE's rejection—without a specific reason—suggests it either did not support the proposed algorithms or detected an anomaly. From a security perspective, it is preferable for the UE to reject a security context it cannot validate or support, rather than accept potentially insecure parameters. Therefore, the UE's action aligns with secure behavior as defined by 3GPP, as it avoids establishing a security context under uncertain or unsupported conditions, even if the rejection cause is unspecified. 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. However, the AMF then sent another "security mode command" message, this time protected with integrity but specifying the ciphering algorithm as 5G-EA0 (null encryption) and the integrity algorithm as 128-5G-IA2, with the security header indicating the use of the 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 the 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 valid reason to use null encryption (5G-EA0), which is generally not recommended for normal operation due to the lack of confidentiality protection. The UE's rejection of the security mode command that attempted to use null encryption, despite the availability of a security context, aligns with the security principles of 3GPP, which prioritize the confidentiality and integrity of user data and signaling. By refusing to accept a downgrade to null encryption after security establishment, the UE demonstrates secure behavior, preventing potential security vulnerabilities such as ciphering algorithm downgrade attacks. Therefore, the UE's action in this scenario was secure. Secure

74	74	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03b3 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11993098258972168 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12021493911743164 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3277699947357178 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then responded with a Security Mode Command. This command was sent as a protected message, indicating that the AMF attempted to establish NAS security using the negotiated ciphering (128-5G-EA3) and integrity (128-5G-IA2) algorithms, with the security header set to "integrity protected with new security context." Upon receiving this, the UE rejected the Security Mode Command, sending a Security Mode Reject message with the cause "unspecified." According to the 3GPP 5G standard, a UE is expected to reject a Security Mode Command if it detects any issues such as unsupported algorithms, mismatched security contexts, or other inconsistencies that could compromise security. The fact that the UE did not proceed with the security context establishment and instead rejected the command—rather than accepting potentially insecure parameters—demonstrates a secure and standards-compliant behavior. The UE's refusal to accept the security context without specifying a reason (using "unspecified") is also allowed by the standard, especially in test or ambiguous situations. Therefore, the UE's actions were secure, as it did not accept a potentially insecure or invalid security context. Secure

75	75	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0392 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.4745960235595703 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4750940799713135 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.47630810737609863 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Security Mode Command message. The Security Mode Command was sent as a protected message, utilizing the negotiated ciphering (5G-EA5) and integrity (128-5G-IA1) algorithms, and the security header indicated that it was integrity protected with a new security context. However, the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard, after the 5G-AKA is completed, the AMF initiates the NAS security context setup by sending a Security Mode Command, and the UE is expected to respond with a Security Mode Complete message if it accepts the proposed security algorithms and context. The absence of any response from the UE is not compliant with the standard, as it leaves the security context establishment incomplete and could potentially expose the session to security risks, such as replay or downgrade attacks, since the mutual agreement on security parameters is not finalized. Therefore, the UE's action in this scenario is considered insecure, as it failed to properly complete the security context establishment as required by 3GPP specifications. 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 for the SUCI (Subscription Concealed Identifier) in plain (unencrypted) NAS message format, as the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G security standards, the SUCI is a privacy-protected identifier designed to prevent exposure of the permanent subscriber identity (SUPI) over the air, especially before a secure NAS connection is established. The standard mandates that sensitive identifiers like the SUCI or SUPI should not be transmitted in cleartext unless absolutely necessary and only under specific, secure conditions. In this case, the UE did not respond to the AMF's plain (unencrypted) identity request for the SUCI, which aligns with the security principle of not exposing subscriber information before the NAS security context is established. This behavior demonstrates that the UE is adhering to the 3GPP security requirements by refusing to send potentially sensitive information in an unprotected message, thereby protecting the subscriber's privacy and security. Secure

77	77	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0004799365997314453 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20071196556091309 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. In response, the AMF sent an identity request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE then replied with an identity response containing the requested SUCI. Importantly, this exchange occurred before the completion of the 5G-AKA (Authentication and Key Agreement) procedure, meaning that the NAS messages were sent in plain (unencrypted) form. According to the 3GPP 5G security standards, it is expected and required that the initial registration and identity request/response messages, including the transmission of the SUCI, occur before the establishment of a security context (i.e., before 5G-AKA is completed). The SUCI is specifically designed to protect the subscriber's permanent identifier (SUPI) by encrypting it with the home network's public key, ensuring that even when sent in the clear, the subscriber's identity remains protected from interception or replay attacks. Therefore, the UE's action of sending the SUCI in response to a plain identity request prior to security context establishment is compliant with 3GPP security requirements and does not expose sensitive information. 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 subsequently sent another "security mode command" message, this time protected with integrity but specifying the ciphering algorithm as 5G-EA0 (null ciphering), meaning no encryption would be applied to subsequent NAS messages, while integrity protection was set to 128-5G-IA2. Upon receiving this command, the UE responded with a "security mode reject" message, indicating that it rejected the security mode command for an unspecified reason. According to the 3GPP 5G standard (TS 24.501), the use of 5G-EA0 (null ciphering) is only permitted under specific circumstances, such as emergency services or when ciphering is not required, and UEs are generally expected to reject security mode commands that attempt to downgrade security (e.g., by requesting null ciphering) outside of these scenarios. The UE's action to reject the security mode command that would have resulted in unencrypted NAS communication, despite the prior establishment of a security context, demonstrates adherence to the 5G security requirements and protects against potential security downgrades or attacks. Therefore, the UE's behavior in this interaction was secure and in line with 3GPP standards. Secure

79	79	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.1600358486175537 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16031789779663086 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36404991149902344 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was protected using integrity (128-5G-IA2) but specified the use of the null ciphering algorithm (5G-EA0), meaning that subsequent NAS messages would not be encrypted, only integrity protected. The UE responded to this command with a Security Mode Reject message, indicating "Security mode rejected, unspecified." According to the 3GPP 5G standard, after authentication, the UE and network should negotiate security algorithms for both integrity and ciphering. The use of 5G-EA0 (null ciphering) is only permitted under specific circumstances, such as emergency services or when explicitly allowed by the UE's security policy. In normal operation, the UE is expected to reject the use of null ciphering to prevent unencrypted transmission of sensitive information. The UE's action to reject the Security Mode Command when only integrity protection (and no encryption) was offered aligns with the security requirements of the 3GPP standard, as it prevents the establishment of a potentially insecure communication channel. Therefore, the UE's behavior in this scenario was secure and in accordance with the 5G security 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 5G-AKA authentication, the UE initiated a Service Request to the AMF, which is a standard procedure to resume or establish a session. The AMF, under test control, responded with a Configuration Update Command, which was sent as a protected (integrity-protected and possibly encrypted) NAS message using a new security context, as indicated by the security header. The UE, upon receiving this message, replied with a 5GMM Status message indicating "Message type not compatible with the protocol state." According to 3GPP standards, after 5G-AKA, all subsequent NAS messages must be integrity protected and, where required, encrypted. The Configuration Update Command is a valid downlink message, but it must be sent in a protocol state where the UE is able to process it. If the UE receives a message that is not compatible with its current protocol state, the standard-compliant behavior is to respond with a 5GMM Status message indicating the incompatibility, which is exactly what the UE did. This response is a security feature to prevent the UE from acting on potentially malicious or out-of-sequence messages, and it ensures protocol robustness. Therefore, the UE's action was secure and in line with 3GPP 5G standards, as it did not process an unexpected or out-of-state message and instead reported the protocol error as specified. Secure

81	81	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 2222 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.1596660614013672 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1599440574645996 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then replied with a Security Mode Command. The Security Mode Command was sent as a protected message, but the selected ciphering and integrity algorithms were both set to null (5G-EA0 and 5G-IA0), meaning that neither encryption nor integrity protection would be applied to subsequent NAS messages. The security header indicated "integrity protected," but with the null algorithm, this protection is effectively absent. The UE, upon receiving this Security Mode Command, did not respond. According to the 3GPP 5G standard (TS 24.501), the use of null algorithms is only permitted under specific circumstances, and UEs are generally expected to reject or ignore Security Mode Commands that request null algorithms unless explicitly allowed by local policy or configuration. By not responding, the UE avoided establishing a security context with no real protection, thereby preventing a downgrade attack or insecure communication. This behavior aligns with the security principles of the 5G standard, which aims to prevent the use of null algorithms unless absolutely necessary and authorized. 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. The AMF then issued a Security Mode Command, which was protected and specified the use of ciphering algorithm 128-5G-EA3 and the null integrity algorithm 5G-IA0. The security header indicated that the message was integrity protected with a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standard, it is mandatory for both ciphering and integrity protection to be enabled for NAS signaling after authentication, as integrity protection is critical to prevent tampering and replay attacks. The use of the null integrity algorithm (5G-IA0) means that no integrity protection would be applied, which is not compliant with the security requirements of the standard. The UE's decision to reject the Security Mode Command under these circumstances demonstrates adherence to the 3GPP security guidelines, as it refused to proceed with a configuration that would compromise the integrity of its communications. Therefore, the UE's action was secure. Secure
83	83	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 8.89320421218872 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.893432140350342 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a standard step for requesting access to network services. The AMF responded with a service accept message, which, according to the packet capture, was sent as a protected (i.e., integrity protected and/or encrypted) NAS message. However, the UE did not provide any response to this protected downlink message from the AMF. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted to ensure confidentiality and authenticity. The UE is expected to process protected messages from the AMF and respond appropriately. The lack of response from the UE to a protected service accept message indicates that the UE either failed to process the protected message or did not recognize it as valid, which is a deviation from the expected secure behavior as per 3GPP specifications. This failure to respond could expose the UE to potential security risks, such as replay or downgrade attacks, if it were to accept unprotected messages or fail to maintain the required security context. Therefore, based on the observed behavior, the UE's action was not secure according to the 5G standard. Insecure

84	84	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0083 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11982488632202148 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12009406089782715 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3228750228881836 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then responded with a Security Mode Command message. This Security Mode Command was sent as a protected message, indicating that it was integrity protected and encrypted using the negotiated algorithms (128-5G-EA2 for ciphering and 128-5G-IA2 for integrity). The security header indicated that a new security context was being used. Upon receiving this command, the UE responded with a Security Mode Reject message, 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 the message is properly protected. A Security Mode Reject is only expected if the UE detects an issue, such as an unsupported algorithm, an invalid security context, or a failure in message integrity verification. Since the Security Mode Command was sent as protected and the algorithms used are standard, the UE's rejection without a specific cause ("unspecified") suggests that it did not provide a clear, standards-based reason for the rejection. This behavior could be considered insecure, as it may indicate that the UE is not properly handling the security procedures or is failing to provide diagnostic information necessary for secure operation and troubleshooting. In summary, the UE's action to reject the Security Mode Command without a specified reason, despite the message being properly protected, does not align with the expected secure behavior as outlined by 3GPP standards. Insecure

85	85	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.16005301475524902 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16028904914855957 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36393094062805176 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to proceed with protected NAS communication. However, the AMF then sent another "security mode command" message, this time protected, specifying the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, which effectively means no encryption or integrity protection would be applied to subsequent NAS messages. Upon receiving this command, the UE responded with a "security mode reject" message, indicating that it refused to accept the proposed security configuration. According to the 3GPP 5G standard (TS 24.501), the use of null algorithms is only permitted in very specific scenarios (such as emergency services or when explicitly allowed by the UE's security policy), and the UE is expected to reject security mode commands that attempt to downgrade security to null algorithms outside of these cases. The UE's action to reject the security mode command with null algorithms demonstrates adherence to the standard and protects against potential security downgrades or attacks. Therefore, the UE's behavior in this interaction was secure and compliant with 3GPP requirements. Secure

86	86	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered (2) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.15096688270568848 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15124177932739258 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.35789990425109863 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity protection) and was ready to begin protected NAS communication. However, the AMF, under test control, responded with another "security mode command" message, which is not the expected behavior according to the 3GPP 5G standard. Normally, after the UE sends "security mode complete," the security context is established, and further NAS messages should be protected using the agreed algorithms. The UE, upon receiving a second "security mode command" after already completing the security mode procedure, should have rejected or ignored this message, as per 3GPP TS 24.501, which states that the UE must not accept a new security mode command unless a new security context is being established (e.g., after a mobility event or re-authentication). Instead, the UE responded again with a "security mode complete" message, indicating that it accepted the repeated security mode command. This behavior is insecure because it exposes the UE to potential replay or downgrade attacks, where an attacker could attempt to disrupt or manipulate the security context by injecting or replaying security mode commands. The UE should have detected this protocol anomaly and refused to process the second security mode command, thereby maintaining the integrity of the security context as required by the 5G standard. Insecure

87	87	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7935822010040283 UE to AMF UplinkNASTransport, Service request 0.793781042098999 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.9976592063903809 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information), InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.9985220432281494 AMF to UE DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes security context for NAS message protection), the UE sent a Service Request to the AMF. The AMF, under test control, responded with a Deregistration Request message that was integrity protected and ciphered, as indicated by the security header. Upon receiving this protected deregistration request, the UE replied with a 5GMM Status message indicating "Invalid mandatory information," suggesting that the UE detected an issue with the content or structure of the deregistration request. The UE then retransmitted an InitialUEMessage and Service Request. According to 3GPP 5G standards, after security context is established, the UE must verify the integrity and validity of all protected NAS messages. If a message contains invalid mandatory information, the UE is expected to respond with a 5GMM Status message indicating the error, rather than processing the invalid request. This behavior prevents the UE from acting on potentially malicious or corrupted messages, thereby upholding the security of the communication. The UE’s actions—detecting the invalid information and responding with a status message—align with the 3GPP security requirements for handling protected NAS messages. Therefore, the UE’s behavior in this scenario is consistent with secure operation as defined by the 5G standard. Secure
88	88	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.1599421501159668 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1602020263671875 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request 0.36409711837768555 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, but the 5G-AKA authentication procedure was not yet completed. The AMF then sent an identity request for the SUCI (Subscription Concealed Identifier) to the UE in plain (unencrypted) NAS, and the UE responded with an identity response. According to the 3GPP 5G security standard, NAS message encryption and integrity protection are only activated after successful completion of the 5G-AKA authentication and key agreement procedure. Before this point, messages—including identity requests and responses—are transmitted in plain text. The SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) by concealing it, even when sent over an unprotected channel. Therefore, the UE's action of responding to a plain identity request with a SUCI before 5G-AKA completion is compliant with the 3GPP standard and does not expose sensitive information. The UE did not send the SUPI or any unprotected permanent identifier, only the SUCI, which is safe to transmit in the clear. Based on this, the UE's behavior in this scenario is secure according to the 5G standard. Secure

89	89	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.12005400657653809 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12025594711303711 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request 0.3216700553894043 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an authentication response to the AMF, which then replied with an identity request for the SUCI (Subscription Concealed Identifier). The AMF sent this identity request as a plain (unencrypted) message because the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. The UE responded with an identity response, providing the requested SUCI. According to the 3GPP 5G standard, before the completion of 5G-AKA, all NAS messages are exchanged in plain text, and the SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) by concealing it, even when sent over an unprotected channel. Therefore, the UE's action of sending the SUCI in response to a plain identity request before security activation is compliant with the 3GPP standard and does not expose sensitive information. The use of SUCI ensures that the subscriber's privacy is maintained even in the absence of NAS security. Based on this, the UE's behavior in this scenario is secure according to the 5G standard. Secure
90	90	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.11975502967834473 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999011039733887 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request 0.3266119956970215 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 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) in plain (unencrypted) NAS, and the UE responded with an identity response. According to the 3GPP 5G security standard, the SUCI is specifically designed to protect the subscriber's permanent identifier (SUPI) from exposure, even when sent over an unprotected channel, by encrypting the SUPI with the home network's public key. The 5G standard allows the SUCI to be sent in plain NAS before security activation, as it does not reveal the SUPI directly and is considered a privacy-preserving identifier. Therefore, the UE's action of sending the SUCI in response to a plain identity request before 5G-AKA completion is compliant with the 3GPP standard and does not expose sensitive information. The UE did not send the SUPI or any other sensitive identifier in cleartext, and thus its behavior is considered secure in this context. Secure

91	91	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7701981067657471 UE to AMF UplinkNASTransport, Service request 0.7708969116210938 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Illegal UE) 0.9781770706176758 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes security context for encryption and integrity protection), the UE sent a Service Request to the AMF. In response, the AMF (under tester control) sent a Deregistration Request (UE terminated) message, which was properly protected with both integrity and ciphering, as indicated by the security header. The UE then responded with a 5GMM Status message indicating "Invalid mandatory information." According to 3GPP standards (TS 24.501), when a UE receives a NAS message that is integrity protected and ciphered, but contains invalid or unrecognized mandatory information elements, the correct and secure behavior is for the UE to respond with a 5GMM Status message indicating the error. This allows the network to be informed of protocol issues without exposing sensitive information, as the communication remains protected by the established security context. Therefore, the UE's actions—responding with a status message after detecting an invalid protected message—are in line with 3GPP security requirements and do not expose the UE to additional risk. Secure
92	92	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.7997009754180908 UE to AMF UplinkNASTransport, Service request 0.7998991012573242 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 1.0037281513214111 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a standard step for accessing network services. In response, the AMF sent a deregistration request to the UE, with the message being integrity protected and ciphered, indicating that NAS security was active and the message was both encrypted and authenticated as per 3GPP 5G security requirements. The UE then responded with a deregistration accept message, acknowledging the deregistration as requested by the AMF. According to the 3GPP 5G standard, once NAS security is established (after 5G-AKA), all subsequent NAS messages, especially those involving sensitive actions like deregistration, must be protected with both integrity and ciphering. The UE's actions—sending a service request after authentication, and then properly responding to a protected deregistration request with a deregistration accept—are fully compliant with the expected secure behavior outlined in the standard. The UE did not process or respond to any unprotected or suspicious messages, and all its actions were within the secure context established by the 5G-AKA procedure. Therefore, based on the observed interaction and adherence to 3GPP security requirements, the UE's actions were secure. Secure

93	93	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 2222 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (UE security capabilities mismatch) The packet capture during the test using wireshark is: 0.15990400314331055 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16019105911254883 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3639252185821533 UE to AMF UplinkNASTransport, Security mode reject (UE security capabilities mismatch) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, 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 parameters. However, the AMF subsequently sent another "security mode command" message, this time protected and specifying the use of ciphering algorithm 5G-EA4 and integrity algorithm 5G-IA0 (null integrity). Upon receiving this, the UE responded with a "security mode reject" message, citing a "UE security capabilities mismatch." According to the 3GPP 5G standard, the use of a null integrity algorithm (5G-IA0) is generally not recommended for normal operation, as it means that the integrity of NAS messages is not protected, potentially exposing the UE to security risks such as message tampering or replay attacks. The UE, by rejecting the security mode command due to the mismatch (specifically, the lack of integrity protection), is acting in accordance with the standard's security requirements, which mandate that the UE should not accept a security configuration that does not meet its minimum security capabilities or requirements. This behavior ensures that the UE does not operate in a potentially insecure state and upholds the integrity of the communication. Therefore, the action taken by the UE was secure and compliant with 3GPP specifications. 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 InitialUEMessage containing a Registration Request to the AMF. In response, the AMF sent an Identity Request message, specifically requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE then replied with an Identity Response containing the requested SUCI. Importantly, this exchange occurred before the completion of the 5G-AKA authentication procedure, meaning that NAS security (encryption and integrity protection) had not yet been established, and the messages were sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), it is expected and required that the initial registration and identity request/response procedures, including the transmission of the SUCI, occur before NAS security is activated, as the network needs to identify the UE before authentication and key agreement can be performed. The SUCI is specifically designed to protect the subscriber's permanent identity (SUPI) by encrypting it with the home network's public key, ensuring that even when sent in the clear, the subscriber's privacy is maintained. Therefore, the UE's action of sending the SUCI in response to a plain identity request before 5G-AKA completion is compliant with the 3GPP standard and does not expose sensitive information. 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 and security setup, the UE initiated a service request to the AMF, which is a standard procedure for requesting network services. In response, the AMF sent a deregistration request (UE terminated) to the UE, and this message was integrity protected and ciphered, indicating that it was sent under an established security context. The UE, upon receiving this protected deregistration request, responded with a deregistration accept message, thereby following the protocol as specified by 3GPP. According to the 3GPP 5G NAS protocol, the UE is required to process and respond to protected NAS messages, even if the message type is unexpected or not compatible with the current protocol state, as long as the message is properly protected (integrity protected and ciphered) and the security context is valid. The UE did not process or respond to any unprotected or suspicious messages, and all communication after 5G-AKA was encrypted as required. Therefore, the UE's actions were in line with the security requirements of the 5G standard, as it only accepted and responded to protected messages and did not expose itself to any known security risks in this interaction. 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 and AMF engaged in NAS communication where, after the initial NAS steps, the UE sent an identity response, and the AMF subsequently issued another identity request, specifically requesting the SUCI (Subscription Concealed Identifier). The UE responded with another identity response. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established, and all messages—including the identity response containing the SUCI—were sent in plain (unencrypted) form. According to the 3GPP 5G standard, the SUCI is designed to protect the subscriber's permanent identifier (SUPI) by concealing it, even when sent over an unprotected channel before authentication and key agreement are complete. The UE's action of providing the SUCI in response to a plain identity request before 5G-AKA is completed is compliant with the standard, as the SUCI is specifically intended for this purpose and does not expose the SUPI. Therefore, the UE's behavior in this scenario is considered secure according to 3GPP specifications. Secure

97	97	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03965497016906738 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0398409366607666 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24122309684753418 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS steps and sent an identity response to the AMF, after which the AMF sent another identity request for the SUCI (Subscription Concealed Identifier). The UE responded with another identity response. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard, the UE is required to respond to identity requests from the AMF even before security activation, but it must never send the cleartext SUPI (Subscription Permanent Identifier); instead, it should send the SUCI, which is a privacy-preserving, encrypted version of the SUPI. In this test, the UE responded to the AMF's identity request with an identity response, and the packet capture shows that this exchange occurred in plain (unencrypted) NAS messages, as expected before 5G-AKA completion. As long as the UE provided only the SUCI (and not the SUPI) in its identity response, its actions are compliant with the 3GPP standard and maintain the intended level of privacy and security for this stage of the protocol. Therefore, the UE's behavior in this interaction is considered secure according to the 5G standard. Secure
98	98	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.798314094543457 UE to AMF UplinkNASTransport, Service request 0.7985830307006836 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command 1.0063400268554688 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA (authentication and key agreement), the UE sent a Service Request to the AMF, which is a standard procedure to resume or establish a session. The AMF then responded with a Configuration Update Command, which was sent as a protected (integrity-protected) NAS message using a new security context, as indicated by the security header. Upon receiving this message, the UE replied with a 5GMM Status message indicating "Message type not compatible with the protocol state." According to the 3GPP 5G NAS protocol (TS 24.501), the UE is required to check the validity and compatibility of received NAS messages with its current protocol state. If the UE receives a message that is not compatible with its current state, it should respond with a 5GMM Status message, as was observed in this test. This behavior ensures that the UE does not process potentially invalid or malicious messages, thereby maintaining protocol integrity and security. The UE's response demonstrates adherence to the 3GPP standard and proper handling of unexpected or out-of-sequence messages, which is a critical aspect of secure communication in 5G networks. Therefore, the action taken by the UE was secure. Secure

99	99	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.5202081203460693 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5204141139984131 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. The AMF then responded with a Downlink NAS Transport message containing a Service Accept, which was sent as a protected (i.e., integrity protected and/or ciphered) message. However, the UE did not respond to this protected Service Accept message from the AMF. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, ciphered to ensure confidentiality and authenticity. The fact that the UE did not respond to a protected Service Accept message suggests that it may not have accepted or processed the message, possibly due to an inability to verify its integrity or decrypt it, or due to a protocol error. From a security perspective, this behavior is actually in line with the 3GPP standard: the UE should not process or respond to NAS messages that are not properly protected after security activation. Since the Service Accept was protected and the UE did not respond (rather than, for example, responding to an unprotected or tampered message), the UE's action is secure, as it avoids potential security risks such as replay or man-in-the-middle attacks. Secure
100	100	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 92 UE provided: No response The packet capture during the test using wireshark is: 0.4685640335083008 UE to AMF UplinkNASTransport, Registration complete 0.4687800407409668 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Insufficient user-plane resources for the PDU session) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after 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 would be protected (i.e., integrity protected and ciphered). The AMF then sent a protected "GMM Status" message to the UE, with a 5GMM cause value of 92, which corresponds to "Insufficient user-plane resources for the PDU session." According to the 3GPP 5G standard (TS 24.501), upon receiving a protected GMM Status message, the UE is not required to respond, especially if the message is not related to an ongoing procedure or does not require corrective action from the UE. The UE's lack of response in this context is compliant with the standard, as the GMM Status message is informational and does not mandate a reply. Furthermore, since all messages after 5G-AKA were protected, the UE maintained the required security for NAS communication. Therefore, the UE's actions were secure and in accordance with 3GPP specifications. Secure

101	101	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 4.873120069503784 UE to AMF SACK (Ack=7, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 4.873471021652222 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is a typical step in establishing a PDU session. The AMF then responded with a Security Mode Command, which was properly protected using the negotiated cipher (128-5G-EA3) and integrity (128-5G-IA2) algorithms, and the security header indicated that a new security context was being used. According to the 3GPP 5G standard, upon receiving a Security Mode Command that is integrity protected with a new security context, the UE is expected to verify the message, apply the new security context, and respond with a Security Mode Complete message to confirm acceptance of the security parameters. However, in this test, the UE did not respond at all to the Security Mode Command. This lack of response is not compliant with the 3GPP standard, as it leaves the security procedure incomplete and could indicate a failure to properly handle protected messages or to establish a secure context. Such behavior could expose the UE to security risks, such as replay or downgrade attacks, or simply result in a failed session setup. Therefore, based on the 3GPP standard and the observed behavior, the UE's action in this scenario was insecure. Insecure

102	102	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.7492289543151855 UE to AMF UplinkNASTransport, Service request 0.749459981918335 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.9532349109649658 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using the null cipher (5G-EA0) and null integrity (5G-IA0) algorithms, but with the security header indicating "Integrity protected with new security context (3)." Upon receiving this, the UE responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G standard, after 5G-AKA, the Security Mode Command should negotiate and activate proper ciphering and integrity protection algorithms (not the null algorithms) to ensure confidentiality and integrity of NAS messages. The use of 5G-EA0 and 5G-IA0 (null algorithms) means that the messages are not actually protected, which is only allowed in very limited scenarios (e.g., emergency services or specific test cases). The UE correctly identified that the Security Mode Command from the AMF was invalid due to the use of null algorithms in a context where security should be enforced, and responded with a status message indicating the error. This behavior aligns with the 3GPP standard, as the UE is expected to reject or report invalid or insecure security configurations. Therefore, the UE's action was secure, as it did not accept an insecure security context and properly reported the issue. Secure
103	103	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5199828147888184 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5202269554138184 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending a Deregistration Request (UE terminated) message back to the UE. The Deregistration Request from the AMF was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered, as required by the 3GPP 5G security standards after authentication is complete. Notably, the UE did not respond to the Deregistration Request. According to 3GPP TS 24.501, upon receiving a protected Deregistration Request, the UE is expected to process the message and respond with a Deregistration Accept message, unless there is a valid reason (such as message integrity failure or decryption error) not to do so. The lack of any response from the UE, despite the message being properly protected, suggests that the UE did not follow the expected protocol behavior. This could indicate a security or implementation issue, as the UE should at least respond or provide an error if it cannot process the message. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure, as it failed to properly handle a protected and valid NAS message. Insecure

104	104	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5198929309844971 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5201320648193359 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (LADN not available) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which was followed by the AMF sending a Deregistration Request (UE terminated) message back to the UE. The Deregistration Request from the AMF was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered, as required by the 3GPP 5G security standards after authentication is complete. The UE, upon receiving this protected Deregistration Request, did not respond. According to the 3GPP specifications, when a UE receives a valid, integrity protected, and ciphered Deregistration Request from the AMF, it is expected to process the request and deregister itself, typically sending a Deregistration Accept message in response. The lack of response from the UE could indicate that it either failed to process the message or did not comply with the expected behavior, which could be a security concern if it means the UE remains registered when it should not be. However, from a strict security perspective, the UE did not send any unprotected or unauthorized messages, nor did it leak any information; it simply did not respond. This behavior is not explicitly insecure, but it is non-compliant with the standard, which could have security implications in a real network. Therefore, while the UE did not act insecurely in terms of exposing data or accepting unprotected messages, its lack of response is not fully aligned with 3GPP requirements for secure deregistration handling. **Insecure**
105	105	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5608680248260498 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5614829063415527 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7653870582580566 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated an Uplink NAS Transport message, which was followed by the AMF sending a Configuration Update Command. The packet capture shows that the Configuration Update Command from the AMF was sent as a protected message, specifically with a security header indicating both integrity protection and ciphering (security header type 2). The UE then responded with a Configuration Update Complete message. According to the 3GPP 5G standard, after the 5G-AKA procedure is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected with both integrity and ciphering to ensure confidentiality and authenticity. The UE's actions—sending the initial message after authentication, receiving and processing a protected configuration update command, and responding appropriately—demonstrate compliance with these security requirements. The UE did not accept or process any unprotected or insecure messages after the security context was established, and all its communications were within the expected secure framework. Therefore, based on the observed behavior and adherence to 3GPP security procedures, the UE's actions were 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 indicated a new security context in the security header. Upon receiving this command, the UE responded with a Security Mode Reject message, citing a "UE security capabilities mismatch." According to the 3GPP 5G standard, the UE is required to verify that the security algorithms proposed by the network in the Security Mode Command are among those it supports and has previously indicated during capability exchange. If there is a mismatch—meaning the network requests algorithms the UE does not support—the UE must reject the security mode command to prevent the establishment of an insecure or unsupported security context. This behavior is explicitly defined to protect the UE from being forced into using weak or unsupported security algorithms, which could compromise the confidentiality or integrity of its communications. Therefore, the UE's action to reject the security mode command due to a capabilities mismatch is in strict compliance with the 3GPP standard and demonstrates secure behavior in the face of a potential security downgrade or misconfiguration. Secure
107	107	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.46604204177856445 UE to AMF UplinkNASTransport, Registration complete 0.466264009475708 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Restricted service area) 0.6700358390808105 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context was established and that subsequent NAS messages should be protected. The AMF then sent a "Deregistration Request (UE terminated)" message, which was integrity protected and ciphered, as indicated by the security header (2), meaning both confidentiality and integrity protection were applied. The UE responded with a "Deregistration Accept (UE terminated)" message, completing the deregistration process. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages must be protected using the established security context. The UE correctly accepted and processed a protected deregistration request and responded appropriately, ensuring that all sensitive signaling was encrypted and integrity protected. There is no indication that the UE accepted or responded to any unprotected or improperly protected messages, nor did it violate any security procedures as outlined by 3GPP. Therefore, the UE's actions were in line with the security requirements of the 5G standard, maintaining the confidentiality and integrity of NAS signaling. Secure

108	108	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.5200989246368408 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5204448699951172 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7219538688659668 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA (authentication and key agreement), the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Configuration Update Command. This downlink message from the AMF was integrity protected and used a new security context, as indicated by the security header. Upon receiving this message, the UE replied with a 5GMM Status message indicating "Message type not compatible with the protocol state." According to the 3GPP 5G standards, after security context establishment, all subsequent NAS messages must be integrity protected and, where required, ciphered. The UE's action to reject the Configuration Update Command with a status message is in line with the standard if the message is unexpected or not allowed in the current protocol state. The use of a protected status message also aligns with the requirement to maintain security after 5G-AKA. Therefore, the UE's behavior—detecting an out-of-sequence or invalid message and responding securely with a status message—demonstrates adherence to the 3GPP security requirements and proper protocol handling. Secure
109	109	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.5209951400756836 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215010643005371 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Unknown) 0.7227599620819092 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes security context for NAS message protection), the UE sent an Uplink NAS Transport message to the AMF, which is a normal procedure. The AMF, under test control, responded with a protected GMM Status message containing a 5GMM cause value of 98. According to 3GPP TS 24.501, the GMM Status message is used to indicate errors or abnormal conditions, but it must only be sent in protocol states where it is valid and expected. In this case, the UE responded with its own GMM Status message, indicating "Message type not compatible with the protocol state." This response from the UE is compliant with the 3GPP standard, as the UE is required to check the validity of received messages against its current protocol state and to reject or report any message that is not compatible. By sending a status message indicating the incompatibility, the UE demonstrates correct protocol behavior and does not process or act upon an unexpected or potentially malicious message. This behavior helps to prevent protocol state confusion or exploitation, thus maintaining the security and integrity of the NAS communication. Therefore, the UE's action in this scenario is secure according to the 3GPP standard. Secure

110	110	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 101 UE provided: No response The packet capture during the test using wireshark is: 0.5881869792938232 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originating) 0.5883810520172119 AMF to UE SACK (Ack=6, Arwnd=106429) , DownlinkNASTransport, 5GMM status (Message not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context was established and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered). Following this, the AMF sent a "5GMM Status" message with cause 101 ("Message not compatible with the protocol state") as a protected downlink NAS message. According to the 3GPP 5G standard (TS 24.501), after the security context is established, the UE is required to process only protected NAS messages and should ignore or silently discard any unprotected NAS messages. In this case, the UE did not respond to the protected "5GMM Status" message from the AMF. This behavior aligns with the 3GPP standard, as the "5GMM Status" message with cause 101 is informational and does not require a response from the UE. The UE's action of not responding, while ensuring that only protected messages are processed after security activation, demonstrates adherence to the security requirements of the 5G standard. Therefore, the UE's behavior in this interaction 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. In response, the AMF sent a Security Mode Command message, which was protected and specified the use of ciphering algorithm 5G-EA5 and integrity algorithm 5G-IA0 (null integrity protection). The security header indicated that the message was integrity protected with a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, citing a "UE security capabilities mismatch." According to the 3GPP 5G standard, the UE is required to verify that the security algorithms proposed by the network are within its capabilities and that integrity protection is not omitted unless explicitly allowed. In this case, the AMF proposed the use of a null integrity algorithm (5G-IA0), which is generally not permitted for user plane or NAS signaling protection except in specific, limited scenarios (such as emergency services or when the UE does not support integrity protection). The UE correctly identified that the proposed security configuration did not match its capabilities or the security requirements and rejected the command, thereby preventing the establishment of a potentially insecure connection. This behavior aligns with the security requirements of the 5G standard, as it ensures that the UE does not accept weak or unsupported security configurations. Secure

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

113	113	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 14.246875047683716 UE to AMF UplinkNASTransport, Service request 14.247098922729492 AMF to UE SACK (Ack=15, Arwnd=106496) , DownlinkNASTransport, Security mode command 14.454866886138916 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command message, which was protected using the negotiated ciphering (128-5G-EA1) and integrity (128-5G-IA2) algorithms, and marked as "integrity protected with new security context." Upon receiving this, the UE replied with a Security Mode Reject message, indicating "Security mode rejected, unspecified." According to the 3GPP 5G standard, after 5G-AKA, the Security Mode Command is used to activate NAS security, and the UE is expected to accept it unless there is a valid reason (such as an unsupported algorithm or a protocol error). The fact that the UE rejected the Security Mode Command with an unspecified cause, despite the message being properly protected and the algorithms being standard, suggests that the UE did not proceed with establishing NAS security as expected. This behavior could expose the UE to potential security risks, as it fails to enter a protected communication state, which is a critical requirement in the 5G security architecture. Therefore, the UE's action in this scenario is not aligned with the secure operation defined by 3GPP standards, as it did not accept the security context and did not provide a specific reason for rejection, potentially leaving the communication vulnerable. Insecure
114	114	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5208940505981445 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215411186218262 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7234148979187012 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE initiated an Uplink NAS Transport message, specifically a PDU session establishment request, to the AMF. The AMF then responded with a Configuration Update Command, which was sent as a protected message—meaning it was both integrity protected and ciphered, as indicated by the security header (value 2). The UE subsequently replied with a Configuration Update Complete message. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected using both integrity protection and ciphering to ensure confidentiality and authenticity. The packet capture confirms that the downlink Configuration Update Command from the AMF was indeed protected, and the UE responded appropriately with the expected acknowledgment. Since the UE only sent messages after the security context was established and responded to protected messages as per the standard, its actions adhered to the security requirements outlined by 3GPP. Therefore, the UE's behavior in this interaction was secure. Secure

115	115	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 14.061744928359985 UE to AMF UplinkNASTransport, Service request 14.062045097351074 AMF to UE SACK (Ack=16, Arwnd=106496) , DownlinkNASTransport, Security mode command 14.26575493812561 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 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. However, upon receiving this 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 security context, and respond with a Security Mode Complete message. Sending a 5GMM Status message with "Invalid mandatory information" suggests that the UE either failed to process the Security Mode Command correctly or detected an issue with the message content, but did not proceed with the expected secure handshake. This behavior could indicate a potential implementation flaw or a security weakness, as the UE did not establish the agreed security context and instead disclosed an error status, which could be exploited in certain attack scenarios. Therefore, based on the 3GPP standard, the UE's action in this context is not fully secure, as it did not follow the prescribed secure procedure after receiving a valid, protected Security Mode Command. 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 0.48129701614379883 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.6844742298126221 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Security Mode Command. This Security Mode Command was sent as a protected message, indicating that it was integrity protected and ciphered using the negotiated algorithms (128-5G-EA2 for ciphering and 128-5G-IA2 for integrity), and the security header indicated the use of a new security context. Upon receiving this, the UE responded with a Security Mode Reject message, specifying "Security mode rejected, unspecified" as the cause. According to the 3GPP 5G standard, after 5G-AKA, the UE is expected to accept the Security Mode Command if the parameters and protection are correct; however, the UE is also permitted to reject the command if it detects any issues, such as mismatched security parameters, integrity check failures, or other security concerns. Since the Security Mode Command was protected and the UE still rejected it, this suggests that the UE detected something it considered invalid or potentially insecure, and thus refused to proceed with establishing the security context. This behavior aligns with the security principles of 3GPP, which prioritize the UE's ability to reject potentially unsafe or non-compliant security procedures to prevent compromise. Therefore, the UE's action in rejecting the Security Mode Command, even with an unspecified cause, is considered secure as it avoids proceeding with a potentially unsafe security context. Secure

117	117	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.5606789588928223 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5618300437927246 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is a typical step in establishing a PDU session. The AMF then responded with a Security Mode Command message, which was sent as a protected (integrity protected and ciphered) message using the negotiated security algorithms (5G-EA5 for ciphering and 128-5G-IA1 for integrity protection) and a new security context, as indicated by the security header value (4). According to the 3GPP 5G standard, after the 5G-AKA procedure, the AMF initiates the NAS security context by sending a Security Mode Command, and the UE is expected to respond with a Security Mode Complete message, confirming that it has activated the new security context. In this test, the UE did not respond to the Security Mode Command. This lack of response is not compliant with the 3GPP standard, as the UE is required to acknowledge and activate the security context to ensure secure NAS communication. The absence of a response could indicate a failure to process the security context or a potential vulnerability, as it leaves the NAS signaling unconfirmed and potentially unprotected. Therefore, based on the 3GPP standard and the observed behavior, the UE's action in this scenario was insecure. Insecure
118	118	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 6.6406471729278564 UE to AMF SACK (Ack=8, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 6.641204118728638 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Configuration update command 6.843037128448486 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated an Uplink NAS Transport message, which was followed by the AMF sending a Configuration Update Command. The packet capture shows that the Configuration Update Command from the AMF was sent as a protected message, specifically with a security header indicating both integrity protection and ciphering (security header type 2). The UE then responded with a Configuration Update Complete message. According to the 3GPP 5G security standards, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be both integrity protected and ciphered to ensure confidentiality and authenticity. The UE's actions in this scenario—responding to a protected Configuration Update Command with a Configuration Update Complete message—are in line with the 3GPP requirements, as the communication occurred only after security activation and the messages were properly protected. Therefore, the UE's behavior demonstrates adherence to the expected security procedures for NAS message exchange in 5G standalone mode. Secure

119	119	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.5208361148834229 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5222671031951904 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.7242951393127441 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Security Mode Command. The Security Mode Command from the AMF specified the use of the 5G-EA0 (null) ciphering algorithm, meaning no encryption would be applied to subsequent NAS messages, while integrity protection was set to 128-5G-IA1. The Security Mode Command was sent as a protected message, and the security header indicated the use of a new security context. Upon receiving this, the UE responded with a Security Mode Reject message, indicating "Security mode rejected, unspecified." According to 3GPP standards (TS 33.501 and TS 24.501), the use of 5G-EA0 (null ciphering) is only permitted under specific, limited circumstances (such as emergency services or when explicitly allowed by the UE's security policy). In normal operation, the UE is expected to reject security mode commands that attempt to establish a null ciphering algorithm, as this would leave NAS messages unencrypted and vulnerable to interception. The UE's action to reject the security mode command in this context demonstrates adherence to the 5G security requirements and protects the confidentiality of its communications. Therefore, the UE's behavior in this scenario was secure. Secure
120	120	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.46767306327819824 UE to AMF UplinkNASTransport, Registration complete 0.46790289878845215 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context was established and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered). The AMF then sent a "Deregistration Accept" message to the UE, which was correctly protected as per the packet capture. However, the UE did not respond to this protected "Deregistration Accept" message from the AMF. According to the 3GPP 5G standard (TS 24.501), upon receiving a protected "Deregistration Accept" message, the UE is not required to send any further NAS message in response; the deregistration procedure is considered complete from the UE's perspective. The UE's lack of response is therefore compliant with the standard and does not indicate any security weakness. The UE only sent messages after the 5G-AKA was completed, ensuring that all subsequent NAS messages were protected, as required. Thus, the UE's actions in this interaction were secure and in line with 3GPP requirements. Secure

121	121	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 1.719182014465332 UE to AMF SACK (Ack=3, Arwnd=106496) , UplinkNASTransport, Authentication response 1.7194299697875977 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS steps and sent an Authentication Response to the AMF, but the 5G-AKA authentication procedure was not yet completed. Immediately after, the AMF sent a Service Reject message with 5GMM Cause 111 (Protocol error, unspecified) in plain (unencrypted) form, as expected since security context establishment (via 5G-AKA) had not occurred. The UE, upon receiving this plain Service Reject message, did not respond further. According to the 3GPP 5G standard, NAS message encryption and integrity protection are only activated after successful completion of the authentication and key agreement (5G-AKA) procedure. Before this, all NAS messages, including Service Reject, are sent in plain text. The UE's behavior—sending the Authentication Response in plain text before security context establishment, and not responding to a plain Service Reject—aligns with the standard and does not expose it to additional risk, as it does not process or act on unauthenticated or unprotected messages beyond what is required. Therefore, the UE's actions in this scenario are consistent with 3GPP security requirements and do not introduce any security vulnerability. Secure
122	122	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003769397735595703 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a Service Reject message, specifically indicating "UE identity cannot be derived by the network" (5GMM Cause 9). Importantly, this Service Reject message was sent in plain (unencrypted) form, which is expected because the 5G-AKA authentication and key agreement procedure had not yet been completed—meaning no security context or encryption keys had been established. According to the 3GPP 5G standard, initial NAS messages, including registration requests and certain reject messages, are permitted to be sent in plain text before authentication is complete. The UE, upon receiving the Service Reject, did not respond further, which is compliant with the standard, as the UE should not proceed with further NAS signaling after receiving a Service Reject with this cause. The UE did not attempt to establish security or send any sensitive information before the 5G-AKA was completed, and it properly ceased communication after the reject. Therefore, the UE's actions were in line with 3GPP security requirements for this stage of the protocol, and no insecure behavior was observed. Secure

123	123	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.03993701934814453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04126906394958496 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.24338102340698242 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication where, after the UE sent an identity response, the AMF issued a Security Mode Command with the security header set to "integrity protected with new security context" and specified ciphering and integrity algorithms. However, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for protecting NAS messages was not yet established. According to the 3GPP 5G standard, the Security Mode Command should only be sent after successful completion of the authentication procedure (5G-AKA), as this ensures that both the UE and the network share the same security context for encryption and integrity protection. Since the AMF sent a protected Security Mode Command before authentication was complete, the UE correctly rejected the command with a "Security mode rejected, unspecified" message. This action by the UE is in line with 3GPP security requirements, as accepting a security mode command without a valid security context could expose the UE to security risks such as replay or man-in-the-middle attacks. Therefore, the UE's behavior was secure and compliant with the standard. Secure
124	124	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03973102569580078 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003596305847168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24200010299682617 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 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 because the 5G-AKA authentication procedure had not yet been completed. The UE responded to this plain identity request by providing another identity response. According to the 3GPP 5G standard, before the completion of 5G-AKA, all NAS messages, including identity requests and responses, are transmitted in plain text, as security context and encryption are not yet established. The UE is expected to respond to identity requests in plain text at this stage, and the use of SUCI (which is a privacy-preserving, concealed form of the subscriber identity) further protects the subscriber's permanent identifier (SUPI) from exposure, even when sent in plain. Therefore, the UE's actions—responding to a plain identity request with a SUCI before 5G-AKA completion—are in line with 3GPP security requirements and do not expose sensitive information. The UE did not act insecurely in this context. Secure

125	125	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00029206275939941406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form, before the 5G-AKA authentication and key agreement procedure was completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should not process or act upon any NAS messages that are received in plain text after the initial registration request, except for a limited set of messages such as Authentication Reject and Security Mode Reject, which are allowed to be sent in plain text before security context is established. In this case, the UE received an Authentication Reject in plain text and did not respond further, which is the expected and secure behavior as per the standard. The UE did not proceed with any further communication or attempt to establish a security context after receiving the reject, thereby preventing any potential exploitation or unauthorized access. This demonstrates that the UE adhered to the 3GPP security requirements by not responding to a plain text Authentication Reject before 5G-AKA completion. 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 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 tester control) sent a "Deregistration Request (UE terminated)" message to the UE, which was integrity protected and ciphered, as indicated by the security header (2). The UE responded appropriately with a "Deregistration Accept (UE terminated)" message, completing the deregistration process. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The UE’s actions—responding only after receiving a protected deregistration request and sending the correct deregistration accept message—demonstrate compliance with the security requirements. The UE did not process or respond to any unprotected or unexpected messages, and all communication after authentication was properly secured. Therefore, based on the observed behavior and adherence to 3GPP security procedures, the UE’s actions in this scenario were secure. Secure

127	127	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.03972792625427246 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an Identity Response message to the AMF, which is a standard step before authentication. However, before the 5G-AKA authentication and key agreement procedure was completed, the AMF sent a Deregistration Accept message to the UE in plain (unencrypted) form. The UE did not respond to this message. According to the 3GPP 5G 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's lack of response to the plain Deregistration Accept message is also compliant, as the standard does not require the UE to respond to a Deregistration Accept, especially when sent before security activation. Therefore, the UE's actions—sending the Identity Response in plain text before authentication and not responding to the Deregistration Accept—are consistent with 3GPP security requirements and do not expose the UE to additional risk in this context. Secure
128	128	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3031 RAND: 00000000000000000000000000000000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Mapped security context ngKSI_KSI: 1 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.03987288475036621 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04013490676879883 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24352788925170898 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an identity response 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 not valid for a real authentication challenge. The UE, upon receiving this malformed and unprotected authentication request, did not proceed with the authentication procedure. Instead, it responded with a 5GMM status message indicating "Invalid mandatory information," effectively rejecting the authentication request due to its invalid content. According to the 3GPP 5G security standards, the UE is required to validate the integrity and correctness of NAS messages, especially before the security context is established (i.e., before 5G-AKA is completed and NAS encryption/integrity protection is activated). The UE must not process or respond to invalid or suspicious authentication requests, particularly those with obviously incorrect parameters or sent in plain text when not appropriate. By refusing to process the invalid authentication request and instead reporting an error, the UE demonstrated correct and secure behavior as per the 3GPP specifications, ensuring that it does not proceed with potentially insecure or malicious authentication procedures. Secure

129	129	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3100 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11980295181274414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12005805969238281 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.321152925491333 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then issued a Security Mode Command, which was integrity protected and indicated the use of the null ciphering algorithm (5G-EA0) and the 128-5G-IA2 integrity algorithm. The security header specified that the message was integrity protected with a new security context. Upon receiving this command, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G security standards, after authentication, the UE and network must agree on both ciphering and integrity algorithms to protect NAS messages. The use of the null ciphering algorithm (5G-EA0) means that no encryption would be applied to subsequent NAS messages, leaving user data vulnerable to eavesdropping. The 3GPP standard (TS 33.501) allows the UE to reject a security mode command if it deems the proposed security algorithms insufficient, especially if only the null ciphering algorithm is offered and the UE policy does not permit unencrypted communication. By rejecting the security mode command under these circumstances, the UE is adhering to best security practices and protecting user confidentiality. Therefore, the UE's action in this scenario is consistent with the 5G security requirements and demonstrates a secure response to a potentially insecure configuration. 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 initial NAS procedures, the UE responded to an identity request with an identity response, as expected. The AMF then sent an authentication request to the UE, but crucially, this message was sent in plain (unencrypted) form before the 5G-AKA procedure was completed. The UE, upon receiving this plain authentication request, replied with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security standards, the authentication and key agreement (5G-AKA) procedure must be completed before any sensitive NAS messages are exchanged in plain text, as this process establishes the security context required for encryption and integrity protection. The UE's refusal to proceed with authentication using a non-5G (i.e., insecure or legacy) method, and its rejection of a plain (unencrypted) authentication request, demonstrates adherence to the 5G security requirements. By not accepting authentication requests that are not protected according to 5G standards, the UE prevents potential security vulnerabilities such as interception or replay attacks. Therefore, the UE's actions in this scenario were secure and compliant with 3GPP 5G security specifications. Secure
131	131	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 26 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00038909912109375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a registration reject message using 5GMM Cause 26 ("Non-5G authentication unacceptable") before the 5G-AKA authentication procedure was completed. The registration reject message was sent in plain (unencrypted) form, which is permitted by the 3GPP 5G standard (TS 24.501) prior to the completion of mutual authentication and key establishment. The UE, upon receiving the registration reject, did not respond further, which aligns with expected behavior since the registration procedure was terminated by the network and no security context had been established yet. According to 3GPP standards, the UE is not required to respond to a registration reject, and it is normal for initial NAS messages (including registration request and reject) to be sent unprotected before authentication is complete. Therefore, the UE's actions were consistent with the 5G security requirements and did not expose it to additional risk in this context. Secure

132	132	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 99 UE provided: No response The packet capture during the test using wireshark is: 0.03979802131652832 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040032148361206055 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service reject (Information element non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). After the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is expected behavior when the network requests the UE's identity. However, before the 5G Authentication and Key Agreement (5G-AKA) procedure was completed—which is necessary to establish NAS security and enable encryption and integrity protection—the AMF responded with a Service Reject message, sent in plain (unencrypted) form with a 5GMM cause value of 99 ("Information element non-existent or not implemented"). The UE, upon receiving this plain Service Reject message before security activation, did not respond further. According to the 3GPP 5G standard, the UE is required to accept and process certain NAS messages, such as Service Reject, even if they are received in plain text prior to the completion of NAS security procedures, since encryption and integrity protection are not yet established at this stage. The UE's action—sending the required Identity Response and then ceasing communication after receiving a Service Reject in plain text—aligns with the expected secure behavior as per the standard, as it did not proceed with any further actions or sensitive exchanges without security being established. Therefore, the UE's behavior in this scenario was secure. Secure
133	133	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3200 RAND: 35353535353535353535353535353535 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.0398869514465332 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040138959884643555 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24263286590576172 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE responded to an identity request from the AMF with an identity response. The AMF then sent an authentication request to the UE, but crucially, this authentication request was sent in plain (unencrypted) form before the 5G-AKA procedure was completed. The UE, upon receiving this plain authentication request, responded with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security standards, specifically TS 33.501, the UE is required to reject authentication requests that do not conform to 5G security requirements, such as those sent in plain text when a native 5G security context is expected. The UE's action to reject the authentication request as "Non-5G authentication unacceptable" demonstrates that it correctly identified a security policy violation and refused to proceed with authentication in an insecure manner. This behavior aligns with the 5G standard's security requirements, as it prevents potential interception or manipulation of sensitive authentication data. Therefore, the UE's action in this scenario was secure. Secure

134	134	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 3 UE provided: No response The packet capture during the test using wireshark is: 0.039869070053100586 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040055036544799805 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service reject (Illegal UE) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). The UE, after completing the initial NAS steps, responded to an identity request by sending an Identity Response message to the AMF. At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that the security context for NAS message encryption and integrity protection was not yet established. Immediately after receiving the Identity Response, the AMF sent a Service Reject message with a 5GMM cause value of 3 ("Illegal UE") in plain (unencrypted) form. 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 successful authentication and key agreement. The UE's behavior—sending the Identity Response in plain text before 5G-AKA and not responding to the Service Reject—aligns with the expected and secure operation as defined by the standard. Therefore, the UE's actions in this scenario were secure and compliant with 3GPP requirements. Secure
135	135	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00067901611328125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.2038860321044922 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a Security Mode Command message that was marked as "protected" but specified the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, and indicated a new security context. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that no valid security context or keys had been established between the UE and the network. Upon receiving the Security Mode Command with null algorithms and without a completed authentication, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G security standards, the UE must not accept a security context that does not provide integrity and confidentiality protection, and it must not proceed with null algorithms unless explicitly allowed under certain conditions (e.g., emergency services). Furthermore, the UE should not accept security mode commands before the successful completion of 5G-AKA, as this would expose it to potential security risks such as man-in-the-middle attacks. By rejecting the security mode command under these circumstances, the UE correctly adhered to the 3GPP security requirements and protected itself from insecure operation. Therefore, the UE's action was secure. Secure

136	136	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA3 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 1.639894962310791 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Identity response 1.6405549049377441 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Security mode command 1.841944932937622 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an identity response to the AMF, the AMF responded with a Security Mode Command message that was integrity protected using a new security context, but specified the use of the null ciphering algorithm (5G-EA0) and an integrity algorithm (128-5G-IA3). Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for establishing encryption and integrity protection was not yet in place. According to the 3GPP 5G security standards (TS 33.501), the Security Mode Command should only be accepted by the UE after successful completion of authentication (5G-AKA), and the use of the null ciphering algorithm (EA0) is only permitted under specific, controlled circumstances. The UE, upon receiving a Security Mode Command with these parameters before authentication was completed and with null encryption, correctly rejected the command with a Security Mode Reject message, citing an unspecified reason. This behavior aligns with the 3GPP security requirements, as the UE must not accept security mode commands that could compromise the confidentiality or integrity of its communications, especially before authentication is complete. Therefore, the UE's action was secure and in compliance with the 5G standard. Secure

137	137	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 2f4b62abf69d8352398c608fb3a89563 AUTN: 062d8ab6b7549000811f4ee8b8da8440 ngKSI_TSC: Native security context ngKSI_KSI: 6 UE provided: Authentication response The packet capture during the test using wireshark is: 1.9198977947235107 UE to AMF SACK (Ack=5, Arwnd=106496) , UplinkNASTransport, Authentication response 1.9201328754425049 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Authentication request 2.120612859725952 UE to AMF UplinkNASTransport, Authentication response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF are engaged in the NAS authentication procedure as part of the 5G-AKA process. The UE first sends an authentication response to the AMF, which is expected behavior after receiving a valid authentication request. However, the AMF then sends another authentication request to the UE, and notably, this message is sent in plain (unencrypted) form. The UE subsequently responds with another authentication response. According to the 3GPP 5G security standard, NAS messages exchanged before the completion of 5G-AKA (i.e., before security context establishment) are allowed to be sent in plain text, as encryption and integrity protection are only activated after successful authentication and key agreement. However, the critical point here is that the UE, after already sending an authentication response, accepts and processes a subsequent plain authentication request from the AMF and responds again, even though the authentication procedure should not be repeated in this manner without a valid reason (such as a failed authentication or explicit restart). This behavior could potentially expose the UE to replay or downgrade attacks, as it is not strictly adhering to the expected state machine and security procedures defined by 3GPP. The UE should have rejected or ignored the unexpected second authentication request, especially since it was sent in plain text after an authentication response had already been provided. Therefore, the UE's action in this scenario is considered insecure according to the 3GPP 5G security standard, as it does not properly enforce the expected authentication flow and may be vulnerable to certain attacks. Insecure

138	138	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5089499950408936 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5091559886932373 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7129359245300293 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and security procedures, the UE sent a "Registration Complete" message to the AMF, indicating that the initial registration process was finalized. Immediately following this, the AMF (under test control) sent a "Deregistration Request (UE terminated)" message to the UE, which was protected with both integrity and ciphering, as indicated by the security header (2). The UE responded appropriately with a "Deregistration Accept (UE terminated)" message, also sent under the established security context. 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 integrity protected and, where required, ciphered. The packet capture confirms that the deregistration request from the AMF was indeed protected, and the UE responded as specified by the standard, only after verifying the security of the received message. There is no indication that the UE accepted or responded to any unprotected or unexpected messages, nor did it proceed with deregistration outside of the secure context. Therefore, the UE's actions were in line with the 3GPP security requirements for NAS message protection, demonstrating correct and secure behavior in this scenario. Secure

139	139	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 31303030000000007894d5bcdd550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 7 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00084686279296875 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.2040548324584961 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an initial registration request to the AMF. The AMF, under test control, responded with an authentication request message that was sent in plain (unencrypted) form, with the 5G-AKA authentication procedure not yet completed. The authentication request included a zeroed AUTN and a test RAND, which are not valid values for a real authentication challenge. Upon receiving this message, the UE did not proceed with the authentication response; instead, it sent a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G standard, the UE is required to verify the integrity and validity of NAS messages before acting on them, especially before the security context is established via 5G-AKA. If the authentication request is malformed or contains invalid mandatory fields (such as a zeroed AUTN), the UE should not proceed with authentication and should instead report an error. The UE's action to reject the message and report invalid information, rather than attempting to process or respond to a potentially insecure or malicious authentication request, aligns with the security requirements of the standard. This behavior helps prevent downgrade or spoofing attacks before a secure context is established. Therefore, the UE's response in this scenario was secure. Secure

140	140	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 300068c66b7f000078b48472b0550000 AUTN: 300068c66b7f0000eeb58472b0550000 ngKSI_TSC: Native security context ngKSI_KSI: 1 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007758140563964844 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.20353293418884277 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with an authentication request message that was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed. According to the 3GPP 5G security standard, it is expected that the initial NAS messages, including the registration request and the authentication request, are sent in plain text because security context and keys are not yet established. However, after receiving the authentication request, instead of proceeding with the authentication procedure (i.e., responding with an authentication response), the UE immediately sent a deregistration request (UE originating) to the AMF. This action indicates that the UE refused to proceed with the authentication process, possibly due to detecting an anomaly or policy violation (such as an unexpected or malformed authentication request, or a security parameter mismatch). From a security perspective, this behavior is considered secure and compliant with 3GPP standards, as the UE did not proceed with authentication or establish a security context in a potentially insecure situation, and instead terminated the registration attempt. This prevents the UE from exposing itself to further risk or potential attacks. Therefore, the UE's action in this scenario is in line with secure behavior as defined by the 5G standard. Secure
141	141	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.17494893074035645 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.17513012886047363 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) completed the initial NAS procedures and sent an Authentication Response to the AMF, after which the AMF replied with an Authentication Reject message. Notably, the Authentication Reject was sent as a plain (unencrypted) NAS message, which is expected behavior since the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed—meaning that security context and encryption keys had not been established. According to the 3GPP 5G standard, until the 5G-AKA is successfully completed, all NAS messages, including Authentication Reject, are transmitted in plain text. The UE, upon receiving the Authentication Reject, did not respond further, which is also compliant with the standard, as the UE is expected to abort the registration or authentication process and not proceed with further communication when authentication is rejected. Therefore, the UE's actions—sending the Authentication Response, receiving the plain Authentication Reject, and not responding further—are in line with 3GPP security requirements and do not expose the UE to additional risk in this context. The UE did not process or respond to any potentially malicious or unexpected messages after the authentication was rejected, which is the secure and expected behavior. Secure

142	142	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 35353535353535353535353535353535 AUTN: 3030303030303000ee95abdf8e550000 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.15996193885803223 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16019487380981445 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.3615410327911377 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with another authentication request message, which was sent in plain (unencrypted) form. The UE then responded with an "Authentication failure (Non-5G authentication unacceptable)" message. According to the 3GPP 5G security standards, specifically TS 33.501, the authentication and key agreement (5G-AKA) procedure must be completed before any sensitive NAS messages are exchanged, and messages should not be sent in plain text after the security context is established. In this case, the AMF sent a plain (unencrypted) authentication request after the authentication response, which is not compliant with the standard. The UE correctly identified this as a security violation and rejected the authentication attempt, indicating that non-5G authentication (i.e., authentication not following the 5G-AKA procedure or not properly protected) is unacceptable. This behavior demonstrates that the UE is adhering to the 5G security requirements by refusing to proceed with an insecure authentication process. Therefore, the UE's action was secure and in line with 3GPP standards. 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 initial registration process was finalized. Subsequently, the AMF sent a "Deregistration Request" message to the UE, which was integrity protected and ciphered, as indicated by the security header (2), meaning the message was both encrypted and authenticated according to 3GPP security requirements. The UE, upon receiving this protected deregistration request, did not respond. According to the 3GPP 5G NAS protocol specifications, a UE is required to process and respond to a valid, protected deregistration request from the AMF, typically by sending a "Deregistration Accept" message. The lack of response from the UE to a properly protected and authenticated deregistration request is not compliant with the standard and could indicate a security or protocol handling issue, as it may leave the network and UE in an inconsistent state and could be exploited in certain attack scenarios. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure. Insecure

144	144	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5077369213104248 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5080108642578125 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.7157459259033203 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication and key agreement procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context was established. Following this, the AMF sent a "Configuration Update Command" to the UE, which was protected with both integrity and ciphering, as indicated by the security header (2). The UE then responded with a "Configuration Update Complete" message. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be protected using the established security context—specifically, they must be both integrity protected and ciphered to ensure confidentiality and authenticity. The packet capture confirms that the downlink message from the AMF was indeed protected, and the UE responded appropriately within the secure context. Since the UE only sent messages after the security context was established and responded to protected messages as required by the standard, the actions taken by the UE align with 3GPP security requirements for NAS communication. Therefore, the UE's behavior in this interaction was secure. Secure
145	145_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.15980100631713867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16017889976501465 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3686530590057373 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters (ciphering and integrity algorithms) negotiated during the security mode command. However, the AMF, under test control, responded with another "security mode command" message, which is not the expected behavior according to the 3GPP 5G standard. The UE then responded again with a "security mode complete" message. According to 3GPP TS 24.501, once the UE has accepted the security mode command and sent a "security mode complete," it should not accept or process a subsequent security mode command unless a new security context is established (e.g., after a re-authentication or context loss). The fact that the UE accepted and responded to a second security mode command without a new authentication or context change indicates a deviation from the standard, as this could potentially allow an attacker to manipulate the security context or downgrade security parameters. This behavior exposes the UE to potential security risks, such as replay or downgrade attacks, and does not align with the expected secure operation as defined by 3GPP. Insecure

146	146	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.1601390838623047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037797927856445 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was completed, establishing a security context between the User Equipment (UE) and the Access and Mobility Management Function (AMF). Following this, the UE sent a "security mode complete" message, indicating that it had accepted the negotiated security algorithms and was ready to communicate securely. The AMF then sent a "deregistration accept" message, which was protected (i.e., integrity protected and/or ciphered) as per the established security context. The UE did not respond to the deregistration accept message. According to the 3GPP 5G standard, after the security mode is complete and the security context is active, all subsequent NAS messages must be protected. The UE's action of not responding to a protected deregistration accept message is compliant with the standard, as the deregistration accept is a terminal message in the deregistration procedure and does not require a response from the UE. The UE did not process or respond to any unprotected messages after security was established, and all communication was appropriately protected. Therefore, the UE's actions were secure and in line with 3GPP requirements. Secure
147	147	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.15987586975097656 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16038084030151367 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.3645758628845215 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to use the new security context for NAS message protection. The AMF then sent a "configuration update command" to the UE, which was correctly protected with integrity and ciphering using the new security context, as indicated by the security header. Upon receiving this protected message, the UE responded with a "5GMM status" message, indicating "Message type not compatible with the protocol state." According to the 3GPP 5G NAS protocol (TS 24.501), after the security mode procedure, the UE should only accept certain messages in specific protocol states. If the AMF sends a message that is not compatible with the current state of the UE, the UE is expected to respond with a status message indicating the incompatibility, as a security and protocol compliance measure. This behavior ensures that the UE does not process unexpected or potentially malicious messages, thereby maintaining protocol integrity and security. Therefore, the UE's action of rejecting the configuration update command with a status message is in line with 3GPP security requirements and demonstrates correct and secure protocol behavior. Secure

148	148	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.11970210075378418 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.11996603012084961 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Congestion) 0.3268871307373047 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G-AKA authentication procedure was successfully completed, establishing a secure context between the User Equipment (UE) and the Access and Mobility Management Function (AMF). Following this, the UE sent a "security mode complete" message, indicating that it had accepted the negotiated security algorithms and was ready to use integrity protection and ciphering for subsequent NAS messages. The AMF then 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 within the established security context. According to the 3GPP 5G standard, after the security mode command is completed and the security context is active, all subsequent NAS messages must be integrity protected and, if required, ciphered. The UE's actions—accepting the security mode, responding only after security was established, and sending its deregistration accept message within the protected context—demonstrate compliance with these requirements. There is no indication that the UE accepted or responded to any unprotected or improperly protected messages after security activation. Therefore, based on the observed behavior and adherence to the 3GPP security procedures, the UE's actions were secure. Secure
149	149	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected (1) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.16007494926452637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037607192993164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.364534854888916 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms (5G-EA7 for ciphering and 128-5G-IA2 for integrity protection) and was ready to begin protected NAS communication. However, the AMF, under test control, responded with another "security mode command" message, which is not the expected behavior according to the 3GPP 5G standard (TS 24.501). Normally, after the UE sends "security mode complete," the security context is established, and further NAS messages should be protected using the agreed algorithms. The UE, upon receiving a second "security mode command" after already completing the security mode procedure, should recognize this as an abnormal or potentially malicious event, as the standard does not expect a new security mode command at this stage. The UE, however, responded again with a "security mode complete" message, indicating that it accepted and processed the repeated security mode command without raising an error or rejecting the message. This behavior is insecure because it exposes the UE to potential replay or downgrade attacks, where an attacker could attempt to disrupt or manipulate the security context by injecting additional security mode commands. According to 3GPP standards, the UE should ignore or reject unexpected security mode commands after the security context is established. Therefore, the UE's action in this scenario did not conform to the expected secure behavior as per the 5G standard. Insecure

150	150	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.16013693809509277 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16036486625671387 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.3618440628051758 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, 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. After authentication, the UE sent a "security mode complete" message, indicating that it had successfully negotiated and activated NAS security (integrity protection and ciphering) with the Access and Mobility Management Function (AMF). Subsequently, the AMF sent a "deregistration request" message to the UE, which was protected with both integrity and ciphering, as indicated by the security header. The UE responded with a "deregistration accept" message, completing the deregistration process. Throughout this exchange, all critical NAS messages after authentication were protected, and the UE only responded to a properly secured and authenticated deregistration request. According to the 3GPP 5G standard, the UE is required to ensure that sensitive NAS messages are only accepted and sent over a protected channel after successful authentication and security mode activation. Since the UE followed this procedure—only accepting and responding to a deregistration request that was integrity protected and ciphered after 5G-AKA and security mode activation—the UE's actions align with the security requirements of the 5G standard. Therefore, the UE's behavior in this scenario was secure. Secure
151	151	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00026297569274902344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE initiated a registration request to the AMF, the AMF responded with an identity request for the GUTI (Globally Unique Temporary Identifier). Importantly, this identity request was sent in plain (unencrypted) form, as the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G security standards (TS 33.501), the UE should not disclose sensitive permanent or long-term identifiers (such as SUPI/IMSI) in plain text before NAS security is activated, but it is generally acceptable to respond with a GUTI, as it is a temporary identifier designed for this purpose. However, in this test, the UE did not respond at all to the identity request for the GUTI. This cautious behavior could be interpreted as the UE refusing to send even a temporary identifier over an unprotected channel, which is stricter than the minimum required by the standard but does not violate it. The UE’s action avoids any risk of identifier exposure before security is established, thus erring on the side of caution. Therefore, based on the 3GPP standard and the context of the test, the UE’s action 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 the NAS communication by sending an initial registration request to the AMF, which is a standard procedure in 5G standalone networks. The AMF, under test control, responded with a configuration update command as a downlink NAS message. Notably, this configuration update command was sent as a "protected" message, 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/or encryption) must 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 UE had not yet completed 5G-AKA, it would not have the required keys to process or verify a protected NAS message. The UE, therefore, did not respond to the configuration update command, which aligns with the 3GPP standard's security requirements—rejecting or ignoring protected messages before security context establishment. This behavior prevents potential security vulnerabilities, such as replay or spoofing attacks, that could arise if the UE processed protected messages without proper key material. Thus, the UE's action in this scenario was secure and compliant with the 3GPP 5G security standards. Secure
153	153	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3200 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007700920104980469 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.20126700401306152 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a Security Mode Command that was protected using a new security context, specifying ciphering with 128-5G-EA3 and integrity protection with 5G-IA0 (null integrity). Notably, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary keys for secure NAS message protection had not been established. Upon receiving the Security Mode Command, the UE responded with a 5GMM status message indicating "Invalid mandatory information." According to 3GPP standards, the UE should not accept or process security-protected NAS messages (such as Security Mode Command) before the successful completion of 5G-AKA, as the required security context is not yet valid. The UE's action to reject the Security Mode Command by sending a status message indicating invalid information aligns with the standard's security requirements, as it prevents the establishment of a potentially insecure or unauthenticated security context. Therefore, the UE's behavior in this scenario was secure and compliant with 3GPP specifications. Secure

154	154	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0009160041809082031 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a configuration update command that was integrity protected and ciphered, as indicated by the security header (2). However, the 5G-AKA authentication and key agreement procedure had not yet been completed at this point in the exchange. According to the 3GPP 5G security standards, NAS message protection (integrity and ciphering) must only be applied after successful completion of the 5G-AKA procedure, which establishes the necessary security context and keys. Since the AMF sent a protected message before 5G-AKA was completed, the UE, adhering to the standard, did not respond to this message. This lack of response indicates that the UE correctly refused to process a protected NAS message before security context establishment, thereby preventing potential security vulnerabilities such as replay or downgrade attacks. Therefore, the UE's action was in line with 3GPP security requirements and demonstrated secure behavior in this scenario. Secure
155	155	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00041294097900390625 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. However, before the 5G-AKA authentication and key agreement procedure was completed—which is required to establish NAS security and enable encryption and integrity protection—the AMF responded with a DownlinkNASTransport message carrying a Deregistration Accept, and this message was sent as "protected." According to the 3GPP 5G standard, NAS security (encryption and integrity protection) must not be applied to messages before the successful completion of 5G-AKA, as the necessary security context has not yet been established. The UE, upon receiving a protected (i.e., encrypted or integrity-protected) NAS message before security activation, is expected to ignore or discard such messages, as it cannot verify or decrypt them without the security context. In this test, the UE did not respond to the protected Deregistration Accept message, which aligns with the 3GPP security requirements and demonstrates that the UE did not process potentially spoofed or invalid protected messages before security was established. Therefore, the UE's action was secure and compliant with the 5G standard. Secure

156	156	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007860660552978516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.2037971019744873 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF responded with a Security Mode Command, which was sent as a protected message but specified the use of null ciphering (5G-EA0) and null integrity (5G-IA0) algorithms, and indicated a new security context. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that no security keys had been established between the UE and the network. Upon receiving the Security Mode Command with null algorithms and without a valid security context, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP 5G security standards, the UE must not accept the establishment of a security context with null algorithms unless explicitly allowed by the operator's policy, and it must not proceed with security mode procedures before the completion of 5G-AKA, as this would leave the communication vulnerable to interception and manipulation. The UE's action to reject the Security Mode Command under these circumstances demonstrates adherence to the 3GPP security requirements, as it prevents the establishment of an insecure communication channel. Therefore, the UE's behavior in this scenario was secure. Secure
157	157	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006291866302490234 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. 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 test control, responded with a deregistration request message that was protected with integrity and ciphering (security header type 2), which is only valid after successful 5G-AKA and NAS security mode establishment. According to the 3GPP 5G standard, the UE should only accept and process protected NAS messages after security context is established; before that, it should ignore or discard such messages. In this test, the UE did not respond to the protected deregistration request, indicating that it correctly ignored the message since security had not been established. This behavior aligns with 3GPP security requirements, as processing protected messages before authentication and key agreement would be a security risk. Therefore, the UE's action was secure. Secure

158	158	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03999805450439453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04024100303649902 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF were engaged in NAS communication prior to the completion of the 5G-AKA authentication procedure, which is required to establish NAS security (encryption and integrity protection). After the UE sent an identity response, the AMF issued another identity request, specifically requesting the IMEISV, and sent this request in plain (unencrypted) form. The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), the UE is required to protect sensitive information such as the IMEISV and should not transmit it in plain text before NAS security is activated. By refusing to respond to the AMF's plain (unencrypted) identity request for the IMEISV prior to the completion of 5G-AKA, the UE correctly avoided exposing sensitive information over an unprotected channel. This behavior aligns with the security requirements of the 5G standard, demonstrating that the UE acted securely in this scenario. Secure
159	159	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 13 UE provided: No response The packet capture during the test using wireshark is: 0.03987693786621094 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04032492637634277 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Roaming not allowed in this tracking area) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication where, after the initial steps, the UE sent an Identity Response message to the AMF. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established, and messages were exchanged in plain text. The AMF then sent a GMM Status message with cause 13 ("Roaming not allowed in this tracking area") in plain text, to which the UE did not respond. According to the 3GPP 5G standard, it is expected that before the completion of 5G-AKA, certain NAS messages, including identity procedures and status messages, may be sent unprotected (in plain text), as security context is not yet available. The UE's lack of response to the plain GMM Status message is also compliant, as the standard does not require the UE to respond to a status message, especially when it indicates a terminal condition such as "roaming not allowed." Therefore, the UE's actions—sending the identity response in plain text before security activation and not responding to the status message—are in line with 3GPP security procedures and do not expose the UE to additional risk in this context. Secure

160	160	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.038893938064575195 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039427995681762695 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) completed the initial NAS procedures and sent an Identity Response message to the Access and Mobility Management Function (AMF). At this point, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. The AMF then sent a Configuration Update Command to the UE as a plain (unencrypted and unauthenticated) NAS message, which is not permitted by the 3GPP 5G standard (TS 24.501). According to the standard, certain NAS messages, such as the Configuration Update Command, must be sent with NAS security protection (i.e., after 5G-AKA is completed and security context is established). The UE, upon receiving this plain Configuration Update Command before security activation, did not respond to the message. This behavior aligns with the 3GPP standard, which requires the UE to ignore or discard such messages if they are not properly protected. By not responding, the UE avoided processing a potentially insecure or malicious message, thereby maintaining the integrity and security of the communication as per the standard. Therefore, the UE's action in this scenario was secure. Secure
161	161	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0400080680847168 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04023408889770508 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an Identity Response message to the AMF, which is a typical step before authentication. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed, the AMF sent a Deregistration Accept message to the UE, and this message was sent as "Protected." According to the 3GPP 5G standard, NAS message protection (integrity and encryption) should only be applied after the 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 should not have accepted or processed protected NAS messages, as it would not have the required keys to verify or decrypt them. The UE's lack of response to the protected Deregistration Accept message indicates that it correctly did not process a protected message before security context establishment, which aligns with the 3GPP security requirements. Therefore, 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, the 5G standalone User Equipment (UE) completed the initial NAS steps and sent an Identity Response message to the Access and Mobility Management Function (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 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed at this point in the exchange. According to the 3GPP 5G standard, NAS message protection (encryption and integrity protection) can only be applied after successful completion of 5G-AKA, which establishes the necessary security context and keys. Since the Service Accept message from the AMF was sent as "protected" before 5G-AKA was completed, the UE, following the standard, should not be able to process or respond to this message, as it does not yet possess the required security context. The UE's lack of response to the protected Service Accept message indicates that it correctly adhered to the 3GPP security requirements by refusing to process a protected message before security activation. This behavior prevents potential security vulnerabilities, such as accepting or acting on messages that could be spoofed or manipulated before a secure context is established. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure
163	163	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.039769887924194336 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.0399930477142334 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an Identity Response to the AMF, which is a typical step before authentication. However, before the 5G-AKA authentication and key agreement procedure was completed, the AMF sent a Deregistration Request message to the UE. Notably, this Deregistration Request was sent with a security header indicating that it was both integrity protected and ciphered, even though the 5G-AKA procedure—which establishes the necessary security context for encryption and integrity protection—had not yet been completed. According to the 3GPP 5G standards (TS 24.501), NAS message protection (integrity and ciphering) must only be applied after a valid security context is established via 5G-AKA. Since the UE had not yet completed 5G-AKA, it would not have the keys required to decrypt or verify the integrity of the protected message. The UE, therefore, did not respond to the protected Deregistration Request, which is the correct and secure behavior as per the standard; responding to a message it cannot verify could expose it to security risks such as replay or spoofing 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

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 with the security header set to "Integrity protected with new security context (3)" and specified ciphering and integrity algorithms. However, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for establishing encryption and integrity protection was not yet in place. According to the 3GPP 5G standard, the Security Mode Command should only be accepted by the UE after successful completion of 5G-AKA, as this procedure establishes the keys required for secure communication. Since the AMF sent a Security Mode Command before 5G-AKA was completed, the UE correctly rejected the command with a Security Mode Reject message, citing an unspecified reason. This behavior aligns with the 3GPP standard, as accepting a Security Mode Command without a valid security context would expose the UE to potential security risks, such as key compromise or man-in-the-middle attacks. Therefore, the UE's action in rejecting the Security Mode Command before authentication was completed demonstrates secure and standards-compliant behavior. Secure

165	165	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3100 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 5G- IA0 (null) Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.03973889350891113 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040254831314086914 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.24545598030090332 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE first sent an identity response to the AMF, after which the AMF issued a Security Mode Command in plain (unencrypted) NAS format, as the 5G-AKA authentication procedure had not yet been completed. The Security Mode Command specified the use of ciphering (128-5G-EA2) but set the integrity algorithm to null (5G-IA0), and the message itself was not protected by a security header. In response, the UE sent a Deregistration Request (UE originating) before any security context was established. According to the 3GPP 5G standard, the UE should not accept or process security mode commands that are not integrity protected, and it should not send sensitive messages (such as deregistration requests) in plain text before the completion of 5G-AKA and the establishment of a security context. By sending a deregistration request in plain NAS before security activation, the UE exposed itself to potential security risks, such as interception or manipulation of its messages. This behavior is not compliant with 3GPP security requirements, which mandate that sensitive NAS messages must be protected after authentication and key agreement. Therefore, the UE's action in this scenario was insecure. Insecure
166	166	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.07990884780883789 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response 0.0801239013671875 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with a configuration update command that was integrity protected but not encrypted, as the 5G-AKA procedure had not yet been completed. According to the 3GPP 5G security standards, encryption and integrity protection of NAS messages should only be activated after successful completion of the 5G-AKA authentication and key agreement procedure, which establishes the necessary security context. Since the 5G-AKA was not completed, the UE should not accept or process any NAS messages that are protected with security headers indicating integrity protection or encryption, as the required keys have not been derived yet. The UE's lack of response to the AMF's configuration update command, which was sent with integrity protection before the security context was established, demonstrates correct and secure behavior according to the standard. The UE did not process or respond to a message that was inappropriately protected before authentication was complete, thereby preventing a potential security vulnerability. Secure

167	167	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.07818889617919922 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response 0.07842707633972168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the IMEISV, but this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA procedure had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), the UE should not respond to identity requests for sensitive information such as IMEI or IMEISV if the NAS security context (i.e., encryption and integrity protection) has not been established, as this could expose the UE's permanent identity to interception or replay attacks. In this case, the UE did not respond to the plain identity request for the IMEISV, which aligns with the security requirements of the standard and demonstrates that the UE is protecting its sensitive information until a secure channel is established. Therefore, the UE's action was secure and compliant with 3GPP security guidelines. 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, which is a normal step in the 5G-AKA authentication procedure. However, before the 5G-AKA process was completed (i.e., before security context establishment and NAS security activation), the AMF sent a "service accept" message to the UE, and this message was marked as "protected." According to the 3GPP 5G standard, NAS message protection (encryption and integrity protection) should only be applied after the successful completion of the 5G-AKA procedure, which establishes the necessary security context. Since the 5G-AKA was not completed, the UE should not have accepted or processed protected NAS messages, nor should it have proceeded with further actions such as sending a deregistration request. The UE's action to process a protected "service accept" message and then send a deregistration request before security context establishment indicates a deviation from the expected secure behavior as defined by 3GPP. This could expose the UE to security risks, such as accepting messages from an unauthenticated or malicious AMF. Therefore, the UE's behavior in this scenario is not compliant with the 5G security requirements. Insecure

169	169	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 26 UE provided: No response The packet capture during the test using wireshark is: 0.1594829559326172 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.15969610214233398 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS procedures and sent an Authentication Response to the AMF, but the 5G-AKA authentication procedure was not yet completed. The AMF, under test control, responded with a GMM Status message indicating "Non-5G authentication unacceptable" (5GMM Cause 26), and this message was sent in plain (unencrypted) form. The UE did not respond 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 expected to be sent in plain text, as encryption and integrity protection are only activated after successful authentication and key agreement. Furthermore, the UE is not required to respond to a GMM Status message, especially when it is received before security activation and indicates an authentication failure. By not responding to the plain GMM Status message and not proceeding with further communication before security was established, the UE adhered to the expected security behavior as outlined by 3GPP. This approach prevents the UE from exposing itself to potential security risks before a secure context is in place. Secure
170	170	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.11972379684448242 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999678611755371 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication where, after the initial steps, the UE 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 the necessary security context for NAS message encryption and integrity protection was not yet established. Despite this, the AMF sent a deregistration request to the UE with the security header set to "integrity protected and ciphered," indicating that the message was both encrypted and integrity protected. According to the 3GPP 5G standard, the UE should only accept and process protected NAS messages (i.e., those with integrity protection and ciphering) after the successful completion of the 5G-AKA procedure, as only then are the required keys available. Since the UE did not respond to the protected deregistration request sent before 5G-AKA completion, it correctly followed the 3GPP security requirements by refusing to process a message that was protected before the security context was established. This behavior prevents potential security vulnerabilities, such as accepting messages that could not be properly decrypted or authenticated. Therefore, the UE's action in this scenario was secure. Secure

171	171	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15981698036193848 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16000986099243164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message for the IMEISV in plain (unencrypted) form, rather than as a protected message. The UE, upon receiving this unprotected identity request after security activation, did not respond. According to the 3GPP 5G standard (TS 24.501), once NAS security is established, the UE must only respond to protected (encrypted and integrity-protected) NAS messages and should ignore or reject any subsequent plain NAS messages, especially those requesting sensitive information such as the IMEISV. The UE's refusal to respond to the unprotected identity request demonstrates correct and secure behavior, as it prevents potential exposure of sensitive information over an unprotected channel. This aligns with the security requirements of the 5G standard, ensuring that sensitive data is not transmitted unless the communication is properly secured. Secure
172	172	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15984892845153809 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16009902954101562 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE requesting the GUTI, but this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after "security mode complete"), all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, if required, encrypted. The UE, upon receiving a plain (unencrypted) identity request after security activation, did not respond. This behavior aligns with the 3GPP standard, which specifies that the UE should ignore any NAS messages received in plain format after security activation, as responding to such messages could expose sensitive information and create a security vulnerability. Therefore, the UE's action of not responding to the plain identity request was secure and compliant with the 5G standard. 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, establishing a security context between the User Equipment (UE) and the Access and Mobility Management Function (AMF). Following this, the UE sent a "Security Mode Complete" message, indicating that it had accepted the negotiated security algorithms and was ready to proceed with protected NAS communication. However, the AMF then sent a "Service Reject" message with 5GMM Cause 111 (Protocol error, unspecified), and crucially, this message was sent in plain (unencrypted) form, despite the security context having been established. Upon receiving this unprotected "Service Reject," the UE responded by sending a "Deregistration Request (UE originating)" message. According to the 3GPP 5G standard (TS 24.501), after the security mode is completed, all subsequent NAS messages—including reject messages—must be integrity protected and, if required, ciphered. The UE, upon receiving an unprotected downlink NAS message after security activation, should ignore it and not act upon it, as processing such messages could expose the UE to security risks such as spoofing or denial-of-service attacks. In this case, the UE's action of accepting and responding to an unprotected "Service Reject" message is not compliant with the 3GPP security requirements and exposes it to potential security vulnerabilities. Therefore, the UE's behavior in this scenario is considered insecure. Insecure
174	174	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: c2ada16de5afa04c9abbf0b2aba327aa AUTN: 3030303030303000ee55922b5d550000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.15995287895202637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16016292572021484 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to begin protected NAS communication. However, the AMF then sent an "authentication request" message to the UE in plain (unencrypted) form, even though the security context had already been established and the UE was expecting all subsequent NAS messages to be integrity protected and, if required, encrypted. According to the 3GPP 5G standard (TS 24.501), once the security mode is complete, the UE must only accept further NAS messages that are integrity protected (and, if required, encrypted) using the established security context. The UE, in this case, did not respond to the plain (unprotected) authentication request, which is the correct and secure behavior as per the standard, since accepting or responding to unprotected messages after security activation could expose the UE to replay or downgrade attacks. Therefore, the UE's action of not responding to the unprotected message was secure and compliant with 3GPP requirements. Secure

175	175	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.15975189208984375 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15996503829956055 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to begin protected NAS communication. However, the subsequent "service accept" message sent by the AMF to the UE was transmitted in plain (unencrypted) form, as observed in the packet capture. According to the 3GPP 5G standard (TS 24.501), after the security mode procedure is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, if required, ciphered. The UE, upon receiving a plain (unencrypted) "service accept" message after security activation, is expected to discard the message and not respond, as accepting or processing unprotected NAS messages after security activation would expose the UE to potential security risks such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected "service accept" message, which aligns with the security requirements of the 5G standard. Therefore, the UE's action was secure and compliant with 3GPP specifications. Secure
176	176	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.47094106674194336 UE to AMF UplinkNASTransport, Registration complete 0.47116804122924805 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context had been established and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered). However, the AMF then sent an "Identity Request" message in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier) from the UE. The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), once the NAS security context is established (after 5G-AKA), all subsequent NAS messages, including identity requests, must be integrity protected and ciphered. If the UE receives a plain (unencrypted) NAS message after security activation, it is required by the standard to ignore the message and not respond, as responding could expose sensitive information or allow for certain types of attacks (such as replay or downgrade attacks). Therefore, the UE's action of not responding to the plain identity request after security activation is in strict compliance with the 3GPP security requirements and demonstrates secure behavior. Secure

177	177	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3031 RAND: 1230c172c0fe20b56039f8264c2856d4 AUTN: 2d236d5db431900054adfe579b1ec661 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.4670701026916504 UE to AMF UplinkNASTransport, Registration complete 0.46730613708496094 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, which is the expected behavior. However, the AMF then sent an "Authentication Request" message to the UE in plain (unencrypted) form, even though the security context should have already been established following the completion of 5G-AKA. According to the 3GPP 5G security standards, once 5G-AKA is completed and a security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. The UE, upon receiving a plain (unencrypted) authentication request after security context establishment, did not respond to this message. This behavior aligns with the 3GPP standard, which specifies that the UE must ignore any NAS messages that are not properly protected after security activation. By refusing to respond to an insecure message, the UE demonstrated correct and secure behavior as per the 5G security requirements. Secure
178	178	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 6.593172073364258 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.593342065811157 AMF to UE SACK (Ack=24, Arwnd=106401) , DownlinkNASTransport, Identity request 6.797163009643555 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after 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., integrity protected and ciphered). However, the AMF then sent an "Identity Request" message in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier) from the UE. Instead of responding with the requested identity, the UE immediately sent a "Deregistration Request (UE originating)" message. According to the 3GPP 5G security standards (TS 33.501 and TS 24.501), after 5G-AKA is completed and security is activated, the UE must not accept or respond to any NAS messages that are not integrity protected and ciphered. The UE's action to not respond to the plain identity request and instead deregister itself demonstrates correct and secure behavior, as it avoids exposing sensitive information (such as SUCI) over an unprotected channel and adheres to the security requirements of the standard. This indicates that the UE is robust against potential downgrade or interception attacks that could exploit unprotected NAS messages after security activation. Secure

179	179	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.265115976333618 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2653589248657227 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.469132900238037 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context should have been established and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered) as per 3GPP TS 24.501. However, the AMF then sent a "Configuration Update Command" as a plain (unencrypted and non-integrity protected) NAS message, which is not compliant with the 5G security requirements, since after 5G-AKA, all NAS messages must be protected. The UE, upon receiving this unprotected message, responded with a "Deregistration Request (UE originating)," effectively terminating its registration. This action by the UE demonstrates that it detected the security anomaly (the receipt of a plain NAS message after security context establishment) and took protective action by deregistering itself, rather than processing the insecure message. According to 3GPP standards, the UE is expected to reject or ignore unprotected NAS messages after security activation, and deregistration is a valid defensive response. Therefore, the UE's behavior aligns with the security requirements of the 5G standard and demonstrates secure handling of the situation. Secure
180	180	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.5163559913635254 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.5165369510650635 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.5166728496551514 AMF to UE DownlinkNASTransport, Configuration update command 2.7203638553619385 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication (which establishes NAS security), 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 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 standard (TS 24.501), after NAS security is established via 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where required, encrypted. If the UE receives a plain NAS message after security is activated, it is considered a protocol violation and a potential security threat (e.g., a downgrade or replay attack). The correct and secure behavior for the UE, as specified by the standard, is to reject the message and initiate deregistration to protect itself and the network. In this test, the UE correctly identified the protocol violation and responded by deregistering, thereby demonstrating secure behavior in accordance with 3GPP requirements. Secure

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

182	182	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.5082509517669678 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 0.5084729194641113 AMF to UE SACK (Ack=7, Arwnd=106334) , DownlinkNASTransport, Configuration update command 0.5085830688476562 AMF to UE DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which should indicate that a secure NAS security context was established and subsequent NAS messages should be integrity protected and ciphered according to 3GPP standards (TS 33.501, TS 24.501). However, the AMF responded with a Service Reject message sent in plain (unencrypted and unprotected) form, with a 5GMM cause code 111 (Protocol error, unspecified). The UE, upon receiving this plain Service Reject message, did not respond further. According to 3GPP standards, after 5G-AKA is completed, the UE is required to only accept NAS messages that are integrity protected and ciphered; any plain (unprotected) NAS message received after security mode is established should be ignored and not acted upon. In this test, the UE did not respond to the unprotected Service Reject message, which is the correct and secure behavior as per the standard, since acting on a plain message after security activation could expose the UE to security risks such as spoofing or denial of service. Therefore, the UE's action in this scenario was secure. Secure

183	183	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 35353535353535353535353535353535 AUTN: 3030303030303000eeb598a00f560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5556139945983887 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.555833101272583 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5559549331665039 AMF to UE DownlinkNASTransport, Authentication request 0.7596380710601807 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message, after which the AMF responded with an Authentication Request message that was sent in plain (unencrypted) form. The UE, upon receiving this unexpected plain Authentication Request after 5G-AKA completion, responded by sending a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G security standards, once 5G-AKA is completed and a security context is established, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where required, encrypted. The reception of a plain (unencrypted) Authentication Request after security context establishment is a protocol violation and could indicate a security attack or misconfiguration. The UE's action to deregister itself upon detecting this anomaly aligns with 3GPP security recommendations, which state that the UE should terminate the connection or take protective action if it detects protocol violations or unexpected plain messages after security activation. This behavior helps prevent potential security breaches such as replay or downgrade attacks. Therefore, the UE's response demonstrates adherence to 5G security standards and proper handling of abnormal or insecure network behavior. Secure

184	184	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 4.666133165359497 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 4.66637396812439 AMF to UE SACK (Ack=10, Arwnd=106401) , DownlinkNASTransport, Configuration update command 4.666524171829224 AMF to UE DownlinkNASTransport, Identity request 4.8701331615448 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message, after which the AMF issued an Identity Request message in plain (unencrypted) form, specifically requesting the IMEI. Instead of responding with the requested identity, the UE immediately sent a Deregistration Request (UE originating) to the AMF. According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where confidentiality is required, encrypted. The IMEI is a permanent equipment identifier and is considered sensitive information; the 3GPP standard (TS 33.501) mandates that the IMEI should only be sent in a protected (encrypted) NAS message after security context establishment. In this case, the AMF violated the standard by requesting the IMEI in plain text, which could expose the UE to privacy risks such as device tracking or interception by an attacker. The UE, by refusing to send its IMEI in response to an unprotected request and instead deregistering, demonstrated correct and secure behavior as per 3GPP requirements, protecting its sensitive information from potential exposure. Therefore, the UE's action was in line with the security expectations of the 5G standard. Secure
185	185	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 62 UE provided: No response The packet capture during the test using wireshark is: 2.4262688159942627 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4268429279327393 AMF to UE SACK (Ack=13, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.427194833755493 AMF to UE DownlinkNASTransport, Registration reject (No network slices available) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the UE proceeds with further NAS procedures. Subsequently, the AMF responded with a Registration Reject message, indicating "No network slices available" (5GMM Cause: 62), and this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed, NAS security (encryption and integrity protection) should be activated for all subsequent NAS messages, except for a few specific cases such as certain reject messages sent before security activation. However, in this scenario, since 5G-AKA was already completed, the expectation is that the UE should only accept Registration Reject messages that are integrity protected and ciphered. The UE, in this case, did not respond to the plain Registration Reject message, which aligns with the security requirements of the standard—rejecting unauthenticated or unprotected critical messages after security activation. This behavior prevents potential security attacks such as false base station attacks or message injection. Therefore, the UE's action of not responding to the unprotected Registration Reject message after 5G-AKA completion is compliant with 3GPP security requirements and demonstrates 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, according to the packet capture and summary, was sent as a plain (unencrypted and unauthenticated) NAS message, even though the 5G-AKA procedure had already been completed and security algorithms (5G-EA6 for ciphering and 128-5G-IA1 for integrity) were selected. Upon receiving this plain Security Mode Command, the UE did not proceed with the expected Security Mode Complete message; instead, it immediately sent a Deregistration Request, effectively aborting the session. According to 3GPP 5G standards, after 5G-AKA is completed, the Security Mode Command should be the first message to establish NAS security, and it is allowed to be sent in plain text. However, once the Security Mode Command is received, the UE should only respond if the message is valid and meets security requirements. If the Security Mode Command is received in an unexpected state, with incorrect parameters, or in a way that could indicate a security risk (such as replay or downgrade attack), the UE is expected to abort the procedure to protect itself. In this case, the UE's immediate deregistration upon receiving a plain Security Mode Command after 5G-AKA suggests it detected a potential security issue and took protective action, which aligns with secure behavior as per 3GPP standards. Therefore, the UE's action was secure. Secure
187	187	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 2.197134017944336 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 2.197467088699341 AMF to UE SACK (Ack=11, Arwnd=106334) , DownlinkNASTransport, Configuration update command 2.1975760459899902 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent a Downlink NAS Transport message containing an Identity Request, specifically requesting the IMEISV (International Mobile Equipment Identity and Software Version) from the UE. Notably, this Identity Request was sent in plain (unencrypted) NAS, despite the fact that 5G-AKA had already been completed, which means that NAS security (encryption and integrity protection) should have been activated for all subsequent NAS messages as per 3GPP standards (TS 24.501, section 5.4.3.1). The UE, upon receiving this unprotected Identity Request, did not respond. According to 3GPP specifications, the UE is required to ignore or reject any NAS messages that are not integrity protected and encrypted after security activation, especially when sensitive information such as IMEISV is being requested. By refusing to respond to an unprotected Identity Request after security context establishment, the UE demonstrated correct and secure behavior, protecting its sensitive identity information from potential interception or misuse. Therefore, the UE’s action was in line with 3GPP security requirements and best practices. Secure

188	188	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.8423888683319092 gNB to AMF UEContextReleaseComplete, InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.8428249359130859 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a service request to the AMF, which is a normal procedure for initiating uplink data or signaling. However, the AMF responded with a Deregistration Accept message sent in plain (unencrypted) NAS, and the UE did not respond to this message. According to the 3GPP 5G security standards (TS 33.501), after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The Deregistration Accept message is a NAS message that, after security context establishment, should be protected. The fact that the AMF sent this message in plain is a deliberate test action. The UE, upon receiving a plain (unprotected) NAS message after security context establishment, is required by the standard to discard the message and not process it further. The UE's lack of response indicates that it did not process the unprotected message, which is the correct and secure behavior as per 3GPP requirements. Therefore, the UE's action in this scenario was secure. Secure
189	189	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 8.602246046066284 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.602970123291016 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a standard step to initiate further communication. The AMF then responded with a Security Mode Command, which is intended to establish NAS security by activating ciphering and integrity protection using the negotiated algorithms (5G-EA6 for ciphering and 128-5G-IA2 for integrity). However, the Security Mode Command from the AMF was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages that carry sensitive information or are used to establish security should be protected with integrity and, where applicable, ciphering. The UE, upon receiving a Security Mode Command in plain text after authentication, did not respond. This behavior aligns with the security expectations of the standard, as responding to an unprotected Security Mode Command could expose the UE to security risks such as replay or man-in-the-middle attacks. By refusing to respond, the UE demonstrated secure behavior in accordance with 3GPP requirements, ensuring that it does not proceed with security establishment unless the message is properly protected. 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 successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF sent an authentication request message to the UE, but crucially, this message was sent in plain (unencrypted) form, despite the fact that a native security context had already been established as indicated by the ngKSI_TSC and the completion of 5G-AKA. According to the 3GPP 5G security standards, once the 5G-AKA procedure is completed and a security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted to prevent interception or tampering. The UE, upon receiving a plain (unencrypted) authentication request after security context establishment, did not respond to the AMF. This behavior aligns with 3GPP security requirements, as the UE is expected to reject or ignore messages that do not comply with the required security protections after a security context is in place. By refusing to respond to an improperly protected message, the UE demonstrated secure behavior in accordance with the 5G standard. Secure

191	191_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1010 RAND: 765bcfb5ee4bd70eb854f2deac92aea9 AUTN: 7f72e2496ad28000fd0cf5cd8a2492b7 ngKSI_TSC: Native security context ngKSI_KSI: 4 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 8.671967029571533 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.672221899032593 AMF to UE SACK (Ack=14, Arwnd=106496) , DownlinkNASTransport, Authentication request 8.874675035476685 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF sent an authentication request message in plain (unencrypted) form, even though a native security context had already been established (as indicated by ngKSI_TSC: Native security context and ngKSI_KSI: 4). Upon receiving this plain authentication request, the UE responded with an authentication failure message, specifically stating "ngKSI already in use." According to the 3GPP 5G security standards, once the 5G-AKA procedure is completed and a native 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 expected to reject or not process any further authentication requests that are sent in plain text under an already established security context, as this could be a replay or downgrade attack. By refusing to process the plain authentication request and responding with an authentication failure, the UE correctly adhered to the 3GPP security requirements, thereby protecting itself from potential security threats. This demonstrates that the UE's actions were secure and compliant with the 5G standard. Secure
192	192	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 35.06067895889282 UE to AMF SACK (Ack=27, Arwnd=106496) , UplinkNASTransport, Service request 35.06101393699646 AMF to UE SACK (Ack=36, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a standard step to resume or establish a connection. The AMF then responded with an Identity Request message, specifically requesting the TMSI, but crucially, this message was sent in plain (unencrypted) NAS signaling. According to the 3GPP 5G security standards (TS 33.501), after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where possible, encrypted to prevent exposure of sensitive information and to protect against various attacks, such as identity interception or replay attacks. The UE, upon receiving a plain (unencrypted) Identity Request after 5G-AKA, did not respond. This behavior aligns with the 3GPP security requirements, as the UE is expected to reject or ignore requests for sensitive information (like TMSI) if the request is not properly protected after security activation. By refusing to respond to an unprotected identity request, the UE demonstrated correct and secure behavior, ensuring that sensitive information is not exposed over an unprotected channel. Secure

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

195	195_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 9.680989980697632 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.681249141693115 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Identity request 9.884641170501709 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF issued an identity request for the SUCI (Subscription Concealed Identifier), which was sent in plain (unencrypted) NAS signaling. The UE then responded with an identity response. According to the 3GPP 5G security standards (TS 33.501), after the 5G-AKA procedure is completed, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, where possible, encrypted to prevent exposure of sensitive information. The SUCI is specifically designed to protect the subscriber's permanent identifier (SUPI) from being exposed, even if sent in the clear, but the 5G standard still mandates that, after authentication, NAS messages 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 3GPP security requirements. The correct behavior would have been for the UE to reject or ignore unprotected NAS messages after 5G-AKA completion. Therefore, the UE's action in responding to an unprotected identity request post-authentication is considered insecure according to the 5G standard. Insecure
196	196	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 9.49011492729187 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.490720987319946 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a Service Request to the AMF, which is a standard procedure to resume or establish a connection for data or signaling. The AMF then responded with a Configuration Update Command, which was sent as a protected (secured) downlink NAS message. However, the security header of the message was marked as "Unknown," and the UE did not provide any response to this message. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted. If the UE receives a NAS message with an unknown or invalid security header, or if the message cannot be verified as protected, the UE is required to discard the message and not respond, as a security measure to prevent potential attacks or protocol violations. In this case, the UE's lack of response to a downlink message with an unknown security header aligns with the 3GPP security requirements, as it avoids processing potentially insecure or tampered messages. Therefore, the UE's action in this scenario was secure. Secure

197	197	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005860328674316406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. At this point, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that security context establishment (integrity and ciphering keys) was not yet in place. The AMF, under test control, responded with a DownlinkNASTransport message containing a Deregistration Request, which was sent with a security header indicating that the message was both integrity protected and ciphered. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) can only be applied after successful completion of the 5G-AKA procedure, as the necessary security context is not available beforehand. The UE, upon receiving a protected message before security context establishment, did not respond, which aligns with the 3GPP specification that requires the UE to discard such messages as they cannot be properly decrypted or authenticated. Therefore, the UE's action of not responding to the prematurely protected deregistration request was secure and compliant with the 5G 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 in plain (unencrypted) form, requesting the UE's GUTI. The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after the security mode complete message), all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, if required, encrypted. The UE is expected to ignore or silently discard any NAS messages received in plain (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 mode completion is compliant with the 3GPP standard and demonstrates secure behavior in this context. Secure

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

201	201	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.15867114067077637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15893101692199707 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message for the IMEI in plain (unencrypted) form, which is not compliant with 3GPP standards. According to 3GPP TS 24.501, once NAS security is established, all subsequent NAS messages, including identity requests, must be protected. The UE, upon receiving an unprotected (plain) identity request after security activation, did not respond. This behavior aligns with the 3GPP standard, which specifies that the UE should ignore or discard any unprotected NAS messages after security mode is complete, to prevent potential security breaches such as IMEI disclosure to an attacker. Therefore, the UE's action of not responding to the plain identity request was secure and compliant with the 5G standard. 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 in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier). The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after the security mode complete message), all subsequent NAS messages between the UE and the AMF must be protected (encrypted and integrity protected). If the UE receives a plain (unencrypted) NAS message after security activation, it is required by the standard to discard the message and not respond, as responding to unprotected messages could expose sensitive information and create security vulnerabilities. Therefore, the UE's action of not responding to the plain identity request after security activation is correct and aligns with 3GPP security requirements, demonstrating secure behavior in this context. Secure

203	203	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15087509155273438 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15108299255371094 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that NAS security (encryption and integrity protection) should now be active for subsequent NAS messages. However, the AMF then sent an "identity request" message to the UE requesting the GUTI, but 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"), all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, if required, encrypted. The UE, upon receiving a plain (unencrypted) NAS message after security activation, is expected to ignore or silently discard such messages to prevent potential security risks such as replay or interception attacks. In this test, the UE did not respond to the plain identity request, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior by refusing to process or respond to an insecure message after security activation. Therefore, the UE's action was secure. Secure
204	204	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15074801445007324 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15094995498657227 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In 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 security standards (TS 33.501 and TS 24.501), once NAS security is established (i.e., after the security mode complete), all subsequent NAS messages, especially those requesting sensitive information such as IMEISV, must be protected by encryption and integrity. The UE, upon receiving an unprotected identity request after security activation, did not respond. This behavior aligns with the 3GPP standard, which specifies that the UE should ignore or reject requests for sensitive information if they are not properly protected after security activation. Therefore, the UE's action of not responding to the unprotected identity request was secure and compliant with the 5G standard. Secure

205	205	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4575481414794922 UE to AMF UplinkNASTransport, Registration complete 0.4577751159667969 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context had been established and NAS security should be active. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) NAS. According to the 3GPP 5G standard, once 5G-AKA is completed and a security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) identity request after security activation, did not respond. This behavior aligns with the 3GPP security requirements, as the UE must not process or respond to NAS messages that are not properly protected after security activation. By refusing to respond to an unprotected identity request, the UE prevents potential security breaches such as identity exposure or replay attacks. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure
206	206	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4691789150238037 UE to AMF UplinkNASTransport, Registration complete 0.46941208839416504 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context had been established and NAS security should be active. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) NAS. According to the 3GPP 5G standard, once 5G-AKA is completed and a security context is established, all subsequent NAS messages, especially those involving sensitive information such as subscriber identity, must be protected by NAS security (i.e., encrypted and integrity protected). The UE, upon receiving an identity request for SUCI in plain NAS after security activation, did not respond. This behavior aligns with 3GPP security requirements, as the UE must not disclose sensitive identifiers over an unprotected channel after security is established. By refusing to respond to an insecure request for its SUCI, the UE demonstrated correct and secure behavior as per the standard. Secure

207	207	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 2.019134998321533 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.0193519592285156 AMF to UE SACK (Ack=7, Arwnd=106361) , DownlinkNASTransport, Identity request 3.000807046890259 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context should have been established and all subsequent NAS messages should be protected (i.e., integrity protected and ciphered). However, the AMF then sent an "Identity Request" message in plain (unencrypted) form, requesting the SUCI (Subscription Concealed Identifier) from the UE. According to the 3GPP 5G security standards (TS 33.501 and TS 24.501), once the 5G-AKA is completed and security is activated, the UE must not respond to any NAS messages that are not integrity protected and ciphered, as responding to plain messages after security activation could expose sensitive information and make the UE vulnerable to various attacks (such as replay or man-in-the-middle attacks). In this test, the UE did not respond to the plain "Identity Request" message from the AMF, which is the correct and secure behavior as per the 5G standard. By refusing to respond to an unprotected message after security activation, the UE ensured that it did not leak any sensitive information or compromise its security context. Secure
208	208	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4989509582519531 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.49918699264526367 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context had been established and NAS security should be active. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) NAS, despite the security context being available. The UE did not respond to this request. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed and NAS security is activated, all subsequent NAS messages, including identity requests, must be protected (integrity protected and, if possible, ciphered). The UE is required to ignore or discard any NAS messages received in plain after security activation, as responding to such messages could expose sensitive information and compromise user privacy. Therefore, the UE's action of not responding to the plain identity request after security activation is compliant with the 3GPP standard and demonstrates secure behavior in this context. Secure

209	209	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.48286890983581543 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.48304104804992676 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security procedures had been completed and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered). However, the AMF then sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), after the completion of the 5G-AKA and the establishment of NAS security, the UE expects all subsequent NAS messages to be integrity protected and ciphered. If the UE receives a plain (unencrypted) NAS message after security has been activated, it should treat this as a protocol error and not respond to the message, as responding could expose sensitive information or allow for certain types of attacks (such as replay or man-in-the-middle). In this test, the UE did not respond to the plain "Identity Request" message, which is the correct and secure behavior as per the 3GPP standard. This action prevents the potential leakage of the SUCI or other sensitive information in an unprotected manner. Therefore, the UE's behavior in this scenario was secure. Secure
210	210	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.48984408378601074 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4900491237640381 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context had been established and NAS security should be active. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted) NAS format. According to the 3GPP 5G standard, once 5G-AKA is completed and a security context is established, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) identity request after security activation, did not respond. This behavior aligns with 3GPP security requirements, as the UE is expected to ignore or reject any NAS messages that are not properly protected after security activation, to prevent potential security breaches such as identity exposure or replay attacks. Therefore, the UE's refusal to respond to an unprotected identity request after security context activation demonstrates adherence to the 5G security standard and is considered a secure action. Secure

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

213	213	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.7595288753509521 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.7598080635070801 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with an Identity Request message asking for the SUCI (Subscription Concealed Identifier). Notably, the AMF sent this Identity Request as a plain (unencrypted) message, even though the 5G-AKA procedure had already been completed, meaning that NAS security (encryption and integrity protection) should have been activated. According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages, especially those involving sensitive identifiers like the SUCI, must be protected by NAS security. The UE, upon receiving an unprotected (plain) Identity Request after security activation, correctly did not respond, as replying with a sensitive identifier over an unprotected channel would violate security requirements and potentially expose the subscriber's identity to interception. Therefore, the UE's action of not responding to the unprotected Identity Request was in line with 3GPP security standards and demonstrated secure behavior in this context. Secure
214	214	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.7997701168060303 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.8000459671020508 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a plain (unencrypted) Identity Request message asking for the TMSI. According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted to prevent exposure of sensitive information. The AMF's request for the TMSI was sent in plain text, which is a security risk, but the focus here is on the UE's behavior. The UE, upon receiving an unprotected identity request after security context establishment, did not respond. This is the correct and secure behavior as per 3GPP TS 33.501, which specifies that the UE must not respond to identity requests that are not integrity protected after security activation. By refusing to send its TMSI in response to an unprotected request, the UE prevented potential exposure of its identity and adhered to the security requirements of the standard. Therefore, the UE's action in this scenario was secure. Secure

215	215	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.5246391296386719 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5248539447784424 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5249319076538086 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF issued an Identity Request message, specifically requesting the IMEISV, and sent this message in plain (unencrypted) form. The UE did not respond to this request. According to the 3GPP 5G security standards (TS 33.501), after the completion of 5G-AKA, all subsequent NAS messages exchanged 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 established. By refusing to respond to a plain (unencrypted) Identity Request for the IMEISV after 5G-AKA completion, the UE is adhering to the security requirements and protecting its sensitive information from potential interception. Therefore, the UE's action in this scenario is consistent with 3GPP security standards and demonstrates secure behavior. 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), and this message was sent in plain (unencrypted) form. The UE did not respond to this request. According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The SUCI is a privacy-protected identifier, and the standard mandates that the UE must not send sensitive identifiers such as the SUCI or SUPI in response to a plain (unencrypted) identity request after security has been activated. By refusing to respond to a plain identity request after 5G-AKA completion, the UE is adhering to the 3GPP security requirements and protecting the subscriber's privacy. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure

217	217	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.531268835067749 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5314879417419434 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5316059589385986 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF. Subsequently, the AMF sent an Identity Request message 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, which means that NAS security (encryption and integrity protection) should have been activated for all subsequent NAS messages. According to 3GPP standards (TS 24.501), after the security context is established via 5G-AKA, the UE must not respond to identity requests or other sensitive information requests sent in plain NAS, as this would expose critical device information to potential interception and compromise user privacy. In this test, the UE did not respond to the plain (unencrypted) Identity Request for the IMEISV, which is the correct and secure behavior as per the 3GPP standard, since responding would have violated the security requirements. Therefore, the UE's action in refusing to respond to an unprotected identity request after security activation was both appropriate and secure. 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, which was followed by the AMF sending a Downlink NAS Transport message containing an Identity Request for the TMSI. Notably, this Identity Request was sent in plain (unencrypted) form, despite the fact that 5G-AKA had already been completed, which means that both the UE and the network should have established NAS security (encryption and integrity protection) for subsequent NAS messages. According to the 3GPP 5G standard (TS 24.501), after the security context is established via 5G-AKA, all subsequent NAS messages, including identity requests, must be protected. The UE, upon receiving an unprotected (plain) identity request after security activation, is required by the standard to ignore the message and not respond, as responding to such a message could expose sensitive information to potential attackers. In this test, the UE did not respond to the unprotected identity request, which is the correct and secure behavior as per the 3GPP standard. Therefore, the UE's action was secure. Secure

219	219	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.5992319583892822 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5994939804077148 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the UE proceeds with further NAS signaling. The AMF then sent an Identity Request message to the UE, specifically requesting the TMSI, and crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, once 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where applicable, encrypted to prevent exposure of sensitive information. The UE, upon receiving a plain (unencrypted) Identity Request after security context establishment, is expected to reject the request or not respond, as responding would risk exposing its identity information over an unprotected channel. In this test, the UE did not respond to the plain Identity Request, which aligns with the security requirements of the 3GPP standard and demonstrates that the UE is correctly protecting its identity information post-authentication. Therefore, the UE's action was secure and compliant with the 5G security specifications. Secure
220	220	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.6309528350830078 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.63124680519104 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which then responded with a Downlink NAS Transport message containing an Identity Request for the TMSI. Notably, this Identity Request was sent in plain (unencrypted) NAS, despite the fact that 5G-AKA had already been completed, meaning that security context and NAS encryption keys should have been established. According to the 3GPP 5G standard (TS 24.501), once 5G-AKA is completed and a security context is in place, all subsequent NAS messages—especially those requesting sensitive information such as the TMSI—must be integrity protected and, where possible, encrypted. The UE, upon receiving a plain (unencrypted) Identity Request after security activation, did not respond. This behavior aligns with the 3GPP security requirements, as the UE is expected to ignore or reject requests for sensitive information if they are not properly protected after security context establishment. By refusing to respond to an unprotected identity request, the UE prevented potential exposure of its identity to an attacker who might be attempting to exploit a security lapse. Therefore, the UE's action was secure and compliant with the 5G standard. Secure

221	221	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 8.961992025375366 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.962584972381592 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is a standard step to request access to network services. The AMF then responded with a Service Accept message, but crucially, this downlink message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, specifically TS 33.501, once 5G-AKA is completed, both the UE and the AMF must establish NAS security (encryption and integrity protection) before exchanging further NAS messages, except for a few explicitly allowed exceptions (such as initial registration or authentication messages). The Service Accept message is not one of these exceptions and should be protected. The UE, upon receiving a plain (unencrypted) Service Accept message after security context establishment, is required by the standard to discard the message and not respond, as accepting or acting on unprotected messages at this stage would expose the UE to security risks such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected Service Accept message, which demonstrates correct and secure behavior according to the 3GPP standard. The UE's refusal to process or acknowledge the insecure message upholds the integrity and confidentiality requirements of the 5G system. Secure
222	222	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 8.977952003479004 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.978222846984863 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request to the AMF, which is a standard step in establishing a secure NAS signaling connection. The AMF then responded with a service accept message, but crucially, this downlink message was sent in plain (unencrypted) form. According to the 3GPP 5G standard, once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, encrypted to ensure confidentiality and prevent replay or tampering attacks. The UE, upon receiving a plain (unencrypted) service accept message after authentication, should have rejected the message or at least not proceeded further, as accepting or acting upon unprotected messages at this stage exposes the UE to significant security risks such as man-in-the-middle or replay attacks. In this test, the UE did not respond to the unprotected service accept message, which indicates that it did not accept or process the insecure message. This behavior aligns with the security requirements of the 3GPP standard, as the UE did not compromise its security by accepting or acting on an unprotected message after authentication. Secure

223	223	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 1.0053770542144775 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.0059680938720703 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is the expected behavior for initiating a service after authentication. The AMF then responded with a Service Reject message, indicating a 5GMM Cause value of 9 ("UE identity cannot be derived by the network"), and crucially, this message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, after the completion of 5G-AKA, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted to ensure confidentiality and prevent tampering or eavesdropping. The UE, upon receiving the plain (unencrypted) Service Reject message after authentication, did not respond further. This behavior aligns with the 3GPP security requirements, which specify that the UE should ignore or not act upon unprotected NAS messages received after security context establishment, as these could be spoofed or manipulated by an attacker. By not responding to the unprotected Service Reject, the UE demonstrated correct and secure behavior as per the standard, protecting itself from potential security threats such as denial-of-service or identity spoofing attacks. Secure
224	224	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 9 UE provided: No response The packet capture during the test using wireshark is: 0.9605340957641602 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 0.9612541198730469 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Service reject (UE identity cannot be derived by the network) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is the expected behavior for initiating a service in a 5G standalone network. The AMF, under test control, responded with a Service Reject message, indicating "UE identity cannot be derived by the network" (5GMM Cause 9). Notably, this Service Reject message was sent in plain (unencrypted) form, despite the fact that 5G-AKA had already been completed, which means that both integrity and ciphering keys should have been established and NAS messages should have been protected. According to 3GPP TS 24.501, after successful authentication and security mode command, all subsequent NAS messages, including Service Reject, must be integrity protected and, if possible, ciphered. The UE, upon receiving the unprotected Service Reject, did not respond further. This behavior aligns with the 3GPP standard, which specifies that the UE should ignore or silently discard any NAS messages that are not integrity protected after security activation. By not responding to the unprotected Service Reject, the UE avoided potential security risks such as replay or spoofing attacks. 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 5G-AKA (authentication and key agreement), the UE sent a Service Request to the AMF, which is the expected behavior for initiating a service. The AMF, under test control, responded with a Service Reject message, which was sent in plain (unencrypted) NAS format and included a 5GMM cause code 111 (Protocol error, unspecified). According to 3GPP TS 24.501, once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF should be integrity protected and, if possible, encrypted to ensure confidentiality and integrity of signaling. The UE, upon receiving a plain (unencrypted) Service Reject message after security context establishment, did not respond further. This behavior aligns with the 3GPP standard, which specifies that the UE should ignore or silently discard any NAS messages that are not integrity protected or encrypted after security activation, as accepting such messages could expose the UE to security risks such as spoofing or replay attacks. Therefore, the UE's lack of response to the unprotected Service Reject message demonstrates correct and secure behavior as per the 5G security requirements. Secure
226	226	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 21 UE provided: No response The packet capture during the test using wireshark is: 0.7632501125335693 UE to AMF UplinkNASTransport, Service request 0.7634460926055908 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Service reject (Synch failure) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request message to the AMF, which is the expected behavior for initiating a service. The AMF then responded with a Service Reject message, indicating a 5GMM Cause value of 21 (which corresponds to "synchronization failure"), and crucially, this reject message was sent in plain (unencrypted) form. According to the 3GPP 5G security standards, after the completion of 5G-AKA, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted to prevent interception or tampering. The UE, upon receiving a plain (unencrypted) Service Reject message after security context establishment, did not respond further. This behavior aligns with 3GPP security requirements, which specify that the UE should ignore or silently discard any unprotected NAS messages received after security activation, as these could be spoofed or manipulated by an attacker. By not responding to the unprotected Service Reject, the UE demonstrated correct and secure behavior as per the standard, ensuring that it does not act on potentially malicious or unauthenticated messages. Secure

227	227	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03d2 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.5453281402587891 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5457210540771484 AMF to UE SACK (Ack=7, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5461199283599854 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the UE proceeds with NAS signaling. The AMF then responded with a Security Mode Command, which was sent as a protected (i.e., ciphered and integrity-protected) message, using the specified cipher (5G-EA6) and integrity (128-5G-IA2) algorithms. However, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, after 5G-AKA, the AMF initiates NAS security by sending a Security Mode Command, and the UE is required to process this command and respond with a Security Mode Complete message, confirming the activation of NAS security. The absence of any response from the UE indicates that it failed to process or accept the Security Mode Command, which is a deviation from the standard and could leave the NAS signaling unprotected if the UE continues communication without activating security. This lack of response is considered insecure, as it prevents the establishment of a secure NAS signaling context and could expose subsequent messages to interception or tampering. Insecure

228	228	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00f2 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 2.722198963165283 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.7225029468536377 AMF to UE SACK (Ack=8, Arwnd=106361) , DownlinkNASTransport, Configuration update command 2.722743034362793 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is a normal step in the NAS communication flow. The AMF then responded with a Security Mode Command, which is intended to establish NAS security by activating ciphering and integrity protection for subsequent NAS messages. However, the Security Mode Command sent by the AMF specified null algorithms for both ciphering (5G-EA0) and integrity protection (5G-IA0), and the security header was marked as unknown. Critically, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, the UE is required to reject or ignore Security Mode Commands that attempt to negotiate null algorithms for both ciphering and integrity protection, as this would leave the NAS signaling unprotected and vulnerable to interception or tampering. The UE's lack of response in this case indicates that it did not accept the insecure security configuration proposed by the AMF, which is the correct and secure behavior as per the standard. Therefore, the UE's action in this scenario was secure. 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 user session. The AMF then responded with a Configuration Update Command, but crucially, this downlink NAS message was sent in plain (unencrypted) form, as indicated by the security header value of 0. According to the 3GPP 5G security specifications (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, encrypted to ensure confidentiality and prevent tampering or eavesdropping. The UE, upon receiving a plain (unencrypted) NAS message after security context establishment, is required by the standard to discard the message and not respond, as accepting or processing such a message would expose the UE to potential security risks such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected Configuration Update Command, which demonstrates correct and secure behavior in line with 3GPP requirements. Therefore, the UE's action was secure. Secure

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

231	231	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3100 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 5G-IA5 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.4284870624542236 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4289300441741943 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4293291568756104 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the UE continues with NAS signaling. The AMF then responded with a Security Mode Command message, but crucially, this message was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed, the Security Mode Command is used to establish NAS security (ciphering and integrity protection) between the UE and the AMF. However, the Security Mode Command itself must be sent as a plain message, since NAS security context is not yet established at this point; only after the UE successfully processes this command and responds with a Security Mode Complete message does NAS security become active. In this test, the UE did not respond to the Security Mode Command. According to the standard, the UE is expected to process the Security Mode Command and reply with a Security Mode Complete message, even though the command is sent in plain text. The lack of response from the UE indicates a failure to follow the 3GPP-specified procedure, as the UE should not require the Security Mode Command to be encrypted at this stage. This behavior could leave the UE unable to establish NAS security, potentially exposing it to security risks or causing service failure. Therefore, the action taken by the UE was not in line with the 5G standard and is considered insecure. Insecure
232	232	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.7425761222839355 UE to AMF UplinkNASTransport, Service request 0.7428131103515625 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a normal step to resume or establish a session. In response, the AMF sent an Authentication Reject message in plain (unencrypted) NAS, and the UE did not respond to this message. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted. The Authentication Reject message is a security-critical message and, per the standard, should be integrity protected after security activation. If the UE receives a plain (unencrypted and unprotected) Authentication Reject after security has been activated, it is expected to ignore the message and not respond, as accepting such a message could expose the UE to security risks such as denial-of-service or impersonation attacks. In this test, the UE did not respond to the unprotected Authentication Reject, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior. 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 user session. In response, the AMF sent an Authentication Reject message to the UE, and notably, this message was sent in plain (unencrypted) NAS format. According to the 3GPP 5G security standards (TS 33.501), after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, encrypted. The Authentication Reject message, being a security-critical message, should be protected to prevent security vulnerabilities such as downgrade or replay attacks. In this test, the UE did not respond to the unprotected (plain) Authentication Reject message. This behavior aligns with 3GPP security requirements, which specify that the UE must ignore or silently discard any NAS messages that are not integrity protected after security context establishment. By not responding, the UE demonstrated correct and secure behavior, as it did not accept or process an unprotected message that could have been tampered with or spoofed. Secure
234	234	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.1599588394165039 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.160261869430542 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the TMSI, but this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA authentication procedure had not yet been completed. According to the 3GPP 5G security standards, specifically TS 33.501, the UE should not send sensitive identifying information, such as the TMSI or SUPI, in response to a plain (unencrypted) identity request after the authentication procedure has started, as this could expose the UE to privacy and security risks (e.g., IMSI/TMSI catching attacks). The correct and secure behavior for the UE, as per the standard, is to not respond to such a request until a secure NAS signaling context is established (i.e., after 5G-AKA is completed and NAS security is activated). In this test, the UE did not respond to the AMF's plain identity request, which aligns with the security requirements and demonstrates that the UE is protecting its identity information as expected. Therefore, the UE's action was secure. Secure

235	235	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.11994314193725586 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12015604972839355 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the IMEISV, but this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA procedure had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), the UE should not disclose sensitive permanent identifiers such as the IMEISV over an unprotected (unencrypted) NAS connection, as this could expose the UE to privacy and security risks, such as device tracking or identity theft. The UE, in this case, did not respond to the plain identity request for the IMEISV, which aligns with the security requirements that prohibit sending permanent identifiers before NAS security is activated. This behavior demonstrates that the UE correctly protected its sensitive information by refusing to transmit the IMEISV in the clear, thereby adhering to the 5G security standards. Secure
236	236	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0173 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.15990495681762695 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1602330207824707 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3627040386199951 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. The AMF then sent a Security Mode Command to the UE, but this message was transmitted as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard, after authentication is completed, the Security Mode Command is used to establish NAS security (ciphering and integrity protection) between the UE and the AMF. The UE is expected to only accept a Security Mode Command that is sent as a plain message immediately after authentication, as this is the only point where it is allowed by the standard. However, after receiving the Security Mode Command, instead of responding with a Security Mode Complete message (which would indicate acceptance and activation of the negotiated security algorithms), the UE sent a Deregistration Request (UE originating). This action suggests that the UE did not proceed to activate NAS security and instead terminated the session. This behavior is actually secure and compliant with the 3GPP standard, as the UE did not accept further communication without proper security activation. By refusing to proceed without NAS security being established, the UE protected itself from potential security risks such as replay or man-in-the-middle attacks. Therefore, the UE's action in this scenario was secure. 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 then replied with a Security Mode Command. The Security Mode Command was sent as a protected message, specifying the use of ciphering algorithm 5G-EA5 and integrity algorithm 5G-IA0 (null integrity protection). Notably, the UE did not respond to this Security Mode Command. According to the 3GPP 5G standard, after authentication, the AMF selects and commands the UE to activate specific ciphering and integrity algorithms. The use of 5G-IA0 (null integrity) is generally discouraged except in specific, controlled scenarios, as it means the NAS messages are not integrity protected, potentially exposing the communication to tampering. The UE, upon receiving a Security Mode Command with null integrity protection, is expected to reject the command or not proceed, as accepting it would compromise the security of subsequent NAS messages. In this test, the UE did not respond to the Security Mode Command, which aligns with secure behavior as per 3GPP standards, since it refused to proceed with a configuration that would have left its NAS signaling unprotected. Therefore, the UE's action was secure. Secure
238	238	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03967404365539551 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.03995108604431152 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an identity response to the AMF, and the AMF subsequently sent another identity request, specifically requesting the TMSI, in plain (unencrypted) NAS signaling. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard (TS 24.501), the UE is required to avoid sending sensitive permanent identifiers (such as SUPI or IMSI) in plain text before NAS security is activated, but it may send less sensitive temporary identifiers (like TMSI) if requested. However, the UE in this test did not respond to the AMF's plain identity request for the TMSI. This behavior aligns with a conservative security posture, as the UE is refusing to send even a temporary identifier over an unprotected channel, thereby minimizing the risk of exposing any identifying information before security is established. This approach is more secure than the minimum required by the standard, as it prevents any potential leakage of identifiers, even temporary ones, in the clear. Therefore, the UE's action in this scenario can be considered secure. Secure

239	239	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.04004096984863281 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04024195671081543 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an identity response to the AMF, and subsequently, the AMF issued another identity request, specifically requesting the IMEISV, in plain (unencrypted) NAS signaling. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard (TS 24.501), the UE is required to protect sensitive information such as the IMEISV and should not transmit it in plain text before NAS security is activated. The UE, in this case, did not respond to the AMF's plain (unencrypted) request for the IMEISV, which aligns with the security requirements of the standard, as sending the IMEISV in the clear would expose the UE to privacy and security risks. Therefore, the UE's action of withholding the IMEISV until NAS security is established demonstrates compliance with 3GPP security guidelines and is considered secure behavior. Secure
240	240	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0363 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.12767410278320312 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1279001235961914 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which then replied with a Security Mode Command. Notably, the Security Mode Command was sent as a plain (unencrypted) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), the Security Mode Command is always sent as a plain NAS message, even after authentication, because it is used to establish the NAS security context (i.e., to agree on the ciphering and integrity algorithms to be used for subsequent messages). The UE, upon receiving this plain Security Mode Command, is expected to respond with a Security Mode Complete message, which should be the first NAS message protected with the newly established security context. However, in this test, the UE did not respond at all to the Security Mode Command. This lack of response is not compliant with the 3GPP standard, as the UE is required to process the Security Mode Command and reply accordingly. The UE's inaction could indicate a security flaw or a failure to properly implement the NAS security procedures, as it neither accepted nor rejected the security context, potentially leaving the session in an undefined or vulnerable state. Therefore, based on the 3GPP standard and the expected behavior, the UE's action in this scenario was insecure. Insecure

241	241	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.16009092330932617 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1604149341583252 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to begin protected NAS communication. However, the AMF then sent another "security mode command" message to the UE, which is not the expected sequence according to the 3GPP 5G standard. Normally, after the UE sends "security mode complete," both the UE and the AMF should consider the NAS security context as established, and all subsequent NAS messages should be protected using the agreed ciphering and integrity algorithms. The UE, upon receiving a second "security mode command" after already completing the security mode procedure, did not respond. This lack of response is actually the correct and secure behavior, as per 3GPP TS 24.501, which states that the UE should ignore any further "security mode command" messages once the security context is established, to prevent downgrade or replay attacks. By not responding, the UE avoided a potential security risk where an attacker could attempt to renegotiate or disrupt the established security context. Therefore, the UE's action was in line with the 5G security standard and demonstrated secure behavior. Secure

242	242	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03f3 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.11997199058532715 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12023186683654785 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Authentication Response to the AMF, which is the expected behavior. The AMF then sent a Security Mode Command to the UE, which was protected (i.e., integrity protected and/or ciphered) using the negotiated security algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity protection), as indicated in the test summary. The Security Mode Command is the first NAS message that should be protected after the establishment of NAS security context, as per 3GPP TS 24.501. However, the UE did not respond to the Security Mode Command. According to the 3GPP standard, the UE is required to process the Security Mode Command, verify its integrity, and respond with a Security Mode Complete message if the command is valid. The lack of response from the UE indicates that it either failed to process the protected message or did not recognize the security header, which is not compliant with the standard. This behavior could expose the UE to potential security risks, such as denial of service or failure to establish a secure NAS connection. Therefore, based on the 3GPP standard, the UE's action in this scenario is considered insecure. Insecure

243	243	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0293 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.15967893600463867 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.15994000434875488 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF. Subsequently, the AMF sent a Security Mode Command to the UE, but this message was sent as a plain (unencrypted and unauthenticated) NAS message, as indicated by the security header value of 0. According to the 3GPP 5G standard (TS 24.501), after the completion of 5G-AKA, the Security Mode Command is the critical message that establishes NAS security (ciphering and integrity protection) between the UE and the AMF. The standard mandates that the Security Mode Command must be sent as a plain NAS message, since security context is not yet established at this point. The UE is expected to process this message and respond with a Security Mode Complete message, which will be the first message protected by the newly negotiated NAS security algorithms. In this test, the UE did not respond to the Security Mode Command. This behavior is secure according to the 3GPP standard, as the UE should only accept a plain Security Mode Command immediately after authentication; if the message is received out of sequence, malformed, or in a context where it is not expected, the UE should ignore or silently discard it to prevent potential security risks such as replay or downgrade attacks. Therefore, the UE's lack of response in this scenario is consistent with secure behavior as defined by the standard. Secure

244	244	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0033 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.16002106666564941 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602630615234375 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms (ciphering: 5G-EA0 (null), integrity: 128-5G-IA2). Following this, the AMF sent a "security mode command" message back to the UE, but crucially, this message was sent as a plain (unencrypted and unauthenticated) NAS message, even though the security context had already been established. According to the 3GPP 5G standard (TS 24.501), once the security mode is completed and the security context is active, all subsequent NAS messages between the UE and the AMF must be protected using the agreed integrity and ciphering algorithms. The UE, upon receiving a plain (unprotected) NAS message after security activation, is required by the standard to discard the message and not respond, as accepting or processing such a message could expose the UE to security risks such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected "security mode command" from the AMF, which is the correct and secure behavior as per 3GPP specifications. Therefore, the UE's action was secure. Secure
245	245	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15975403785705566 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16004419326782227 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF replied with an identity request for the IMEISV, but crucially, this request was sent in plain (unencrypted) NAS signaling because the 5G-AKA procedure had not yet been completed. According to the 3GPP 5G security standards (TS 33.501), sensitive information such as the IMEISV should only be transmitted after NAS security (ciphering and integrity protection) is activated, which occurs after successful completion of the 5G-AKA authentication and key agreement procedure. Since the UE did not respond to the AMF's plain (unencrypted) identity request for the IMEISV, it correctly avoided exposing sensitive information over an unprotected channel. This behavior aligns with the security requirements of the 5G standard, which aims to prevent the disclosure of device identities before a secure channel is established. Therefore, the UE's action in this scenario was secure and compliant with 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 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) 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. According to the 3GPP 5G standard, the UE should not respond to identity requests for sensitive identifiers (such as TMSI, SUPI, or GUTI) if the request is received in plain text after the authentication response, as this could expose the UE to identity disclosure attacks. The UE's action of not responding to the plain identity request is therefore in line with 3GPP security recommendations, as it avoids leaking sensitive information before a secure NAS context is established. This behavior demonstrates that the UE is correctly implementing the security requirements of the 5G standard by refusing to send its identity in the clear after authentication has started but before security is activated. Secure
247	247	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.1999650001525879 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.20019102096557617 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE completed the initial NAS procedures and sent an authentication response, the AMF (under your control) sent an Identity Request message to the UE, specifically requesting the IMEISV. Importantly, this Identity Request was sent in plain (unencrypted) NAS, 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 3GPP 5G security standards (TS 33.501 and TS 24.501), the IMEI/IMEISV is considered a sensitive identifier and should only be transmitted over a protected (encrypted) NAS connection, except in very specific and justified cases (e.g., regulatory requirements or emergency services). In this test, the UE did not respond to the plain (unencrypted) Identity Request for the IMEISV, which aligns with the security recommendations to avoid exposing device identifiers before NAS security is activated. This behavior demonstrates that the UE is following best security practices as outlined by 3GPP, by refusing to send sensitive information in the clear. Therefore, the UE's action in this scenario was secure. Secure

248	248	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA3 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.11875295639038086 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11905193328857422 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an authentication response to the AMF, which is the expected behavior. The AMF then sent a Security Mode Command to the UE, which was marked as "Protected" and included the ABBA parameter, ciphering algorithm 128-5G-EA2, and integrity algorithm 128-5G-IA3. However, the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard, after the 5G-AKA is completed, the Security Mode Command is the first NAS message that should be integrity protected (and optionally ciphered, depending on the configuration) using the negotiated algorithms. The UE is expected to verify the integrity of this message, accept the security context, and respond with a Security Mode Complete message if the command is valid. If the security header is "Unknown" or the message cannot be verified, the UE should discard the message and not respond, as a security measure to prevent attacks such as replay or tampering. In this test, since the Security Mode Command's security header was "Unknown" and the UE did not respond, the UE correctly followed the 3GPP security guidelines by refusing to process or acknowledge a potentially insecure or malformed message. This behavior demonstrates that the UE is secure in its communication, as it did not accept or process a message that could not be properly authenticated. Secure
249	249	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.7274200916290283 UE to AMF UplinkNASTransport, Service request 0.7277319431304932 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a standard step to resume or establish a user session. The AMF then responded with a Configuration Update Command, but crucially, this downlink NAS message was sent in plain (unencrypted) form, as indicated by the security header value of 0. According to the 3GPP 5G security specifications (TS 33.501), once 5G-AKA is completed, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, encrypted to ensure confidentiality and prevent tampering or eavesdropping. The UE, upon receiving a plain (unencrypted) NAS message after security context establishment, is required by the standard to discard the message and not respond, as accepting or processing such a message could expose the UE to security risks such as replay or man-in-the-middle attacks. In this test, the UE did not respond to the unprotected Configuration Update Command, which demonstrates correct and secure behavior in line with 3GPP requirements. Therefore, the UE's action 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, and subsequently, the AMF sent another Identity Request asking 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 cleartext before NAS security (ciphering and integrity protection) is established, which only occurs after successful completion of 5G-AKA. The UE, upon receiving a plain (unencrypted) Identity Request for the IMEISV before security activation, did not respond. This behavior aligns with the 3GPP security recommendations, as it prevents the exposure of sensitive device identifiers over an unprotected channel, thereby mitigating the risk of device tracking or identity theft. Therefore, the UE's refusal to respond to the unprotected request demonstrates adherence to the security requirements of the 5G standard. Secure
251	251	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03961300849914551 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039839982986450195 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, and the AMF subsequently sent another Identity Request, specifically requesting the TMSI, in plain (unencrypted) NAS signaling. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard (TS 24.501), the UE is required to respond to identity requests even if NAS security is not activated, but there are important security considerations: the UE should not send sensitive permanent identifiers (such as the SUPI/IMSI) in plain text unless absolutely necessary, and should prefer to send temporary identifiers (like TMSI or GUTI) when possible. In this case, the AMF requested the TMSI, which is a temporary identifier, and the UE did not respond to the plain (unencrypted) identity request. This behavior is more cautious than the minimum required by the standard, as the standard does allow the UE to respond with a TMSI in plain text before security activation, but it is not strictly required to do so. By refusing to send any response in the absence of NAS security, the UE is prioritizing the protection of its identity, even its temporary identity, against potential interception. This conservative approach enhances privacy and security beyond the baseline requirements of the standard, especially in a test or potentially hostile environment. Therefore, the UE's action can be considered secure, as it avoids exposing even temporary identifiers over an unprotected channel. Secure

252	252	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03987598419189453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040084123611450195 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an identity response to the AMF. Subsequently, the AMF 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 in plain text before the establishment of a secure NAS security context, which is only set up after successful completion of 5G-AKA. The UE, upon receiving a plain (unencrypted) identity request for the IMEISV before security activation, chose not to respond. This behavior aligns with 3GPP security recommendations, as it prevents the exposure of sensitive device identifiers over an unprotected channel, thereby mitigating the risk of device tracking or identity theft. Therefore, the UE's refusal to respond to the unprotected identity request demonstrates adherence to security best practices as outlined in the 5G standard. Secure
253	253	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.7599589824676514 UE to AMF UplinkNASTransport, Service request 0.7601721286773682 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF issued an identity request for the UE’s GUTI, but crucially, this identity request was sent in plain (unencrypted) NAS signaling. The UE did not respond to this request. 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 applicable, encrypted. The standard specifically prohibits the AMF from sending identity requests in plain text after security has been established, as this could expose sensitive information to potential attackers. By refusing to respond to an identity request that was not properly protected, the UE adhered to the security requirements of the 5G standard, thereby preventing the possible leakage of its identity information. This behavior demonstrates that the UE correctly enforced the security policy as defined by 3GPP, ensuring that its communication remained secure even in the face of a protocol violation by the network. Secure

254	254	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 6.647611856460571 UE to AMF SACK (Ack=7, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 6.6478259563446045 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Service accept, Unknown code (0x45) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which is the expected behavior as the UE initiates a PDU session establishment request. The AMF, under test control, responded with a Service Accept message, but crucially, this downlink message was sent in plain (unencrypted) NAS, as indicated by the packet capture and the test summary. According to the 3GPP 5G standard (TS 24.501), after the completion of 5G-AKA, both the UE and the AMF must establish NAS security (encryption and integrity protection) before exchanging further NAS messages, except for a few explicitly allowed exceptions (such as certain security mode commands or reject messages). The Service Accept message is not one of these exceptions and must be protected. The UE, upon receiving a plain (unencrypted) Service Accept message after 5G-AKA, should have rejected the message or ignored it, 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 did not respond to the unprotected Service Accept message, which is the correct and secure behavior according to the 3GPP standard, as it did not process or acknowledge an insecure message. Secure
255	255	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 12.160748958587646 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 12.161019086837769 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. In response, the AMF issued an Identity Request message, specifically requesting the IMEI, and crucially, this message was sent in plain (unencrypted) form. The UE did not respond to this request. According to the 3GPP 5G security standards (TS 33.501), after the completion of 5G-AKA, all subsequent NAS messages, including identity requests, must be integrity protected and, where possible, encrypted to prevent exposure of sensitive information such as the IMEI. The IMEI is considered a permanent equipment identifier and should not be transmitted in cleartext after security has been established, as this could expose the UE to privacy risks such as device tracking or profiling. By refusing to respond to an unprotected identity request after security context establishment, the UE is adhering to the 3GPP security requirements and protecting the user's privacy. Therefore, the UE's action in this scenario was secure. Secure

256	256	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 97 UE provided: No response The packet capture during the test using wireshark is: 0.46838808059692383 UE to AMF UplinkNASTransport, Registration complete 0.4686100482940674 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Message type non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context had been established and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered). However, the AMF then sent a "5GMM Status" message with cause 97 ("Message type non-existent or not implemented") in plain (unencrypted and non-integrity protected) form. According to 3GPP TS 24.501, once the NAS security context is established (after 5G-AKA), the UE must ignore any subsequent plain (unencrypted) NAS messages, except for a very limited set of exceptions (such as Service Reject or Deregistration Accept under specific conditions). The "5GMM Status" message is not one of these exceptions. In this test, the UE did not respond to the plain "5GMM Status" message, which is the correct and secure behavior as per the 3GPP standard, since responding to or processing such a message could expose the UE to security risks such as replay or downgrade attacks. Therefore, the UE's action in this scenario was secure. Secure
257	257	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4328169822692871 UE to AMF UplinkNASTransport, Registration complete 0.4330179691314697 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the security context had been established and NAS security should be active. Subsequently, the AMF sent an "Identity Request" message to the UE, requesting the SUCI (Subscription Concealed Identifier), but crucially, this message was sent in plain (unencrypted) NAS. According to the 3GPP 5G standard, once 5G-AKA is completed and a security context is established, all subsequent NAS messages, especially those involving sensitive information such as identity requests, must be protected (i.e., encrypted and integrity protected). The UE, upon receiving an unprotected identity request after security activation, is expected to reject the request or ignore it to prevent potential security breaches, such as identity interception or replay attacks. In this test, the UE did not respond to the unprotected identity request, which aligns with the security requirements of the 3GPP standard, as responding with sensitive information over an unprotected channel would be insecure. Therefore, the UE's action of not responding to the plain identity request after security activation was the correct and 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 initial registration and security setup were finished. Subsequently, the AMF sent a "Deregistration Request" message to the UE, which was transmitted as a plain (unencrypted) message but with a security header indicating "integrity protected and ciphered (2)." The UE then responded with a "Deregistration Request (UE originating)" message. According to the 3GPP 5G standards (TS 24.501), after the 5G-AKA procedure, all subsequent NAS messages exchanged between the UE and the AMF should be both integrity protected and ciphered to ensure confidentiality and integrity of the signaling. The packet capture shows that the AMF's deregistration request was sent as a plain message, which is not compliant with the standard, but since the AMF was under test control, the focus is on the UE's behavior. The UE, upon receiving a plain (potentially insecure) deregistration request, responded with a deregistration request of its own. According to 3GPP standards, the UE should only accept and process NAS messages that are properly protected after security activation; responding to a plain, unprotected message after security is established is considered insecure behavior, as it could allow an attacker to trigger deregistration via a replay or forged message. Therefore, the UE's action in this scenario is not secure according to the 5G standard. Insecure
259	259	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 99 UE provided: No response The packet capture during the test using wireshark is: 0.5207638740539551 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.521324872970581 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Information element non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message to the AMF, which is expected to be encrypted and integrity protected as per 3GPP standards once security has been established. The AMF then responded with a GMM Status message, indicating a 5GMM cause value of 99 ("Information element non-existent or not implemented"), and crucially, this message was sent in plain (unencrypted) form. According to 3GPP TS 24.501, after security mode is established (i.e., after 5G-AKA), all subsequent NAS messages, including status messages, must be integrity protected and, where applicable, encrypted. The UE, upon receiving a plain (unencrypted) NAS message after security activation, is required by the standard to discard the message and not respond to it. In this test, the UE did not respond to the unprotected GMM Status message, which aligns with the 3GPP security requirements and demonstrates correct and secure behavior by the UE. Therefore, the UE's action in this scenario was secure. Secure

260	260	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 101 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5113871097564697 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.511634111404419 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, 5GMM status (Message not compatible with the protocol state) 0.7153670787811279 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security procedures had been completed and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered) as per 3GPP TS 24.501. However, the AMF then sent a "5GMM Status" message with cause 101 ("Message not compatible with the protocol state") in plain (unencrypted and non-integrity protected) format, which is only permitted in very limited circumstances, such as before security activation or when the UE cannot process protected messages. Upon receiving this unprotected status message, the UE responded by sending a "Deregistration Request (UE originating)" message. According to 3GPP standards, after security activation, the UE should generally ignore unprotected NAS messages unless they are explicitly allowed (e.g., certain status messages in specific error conditions). The UE's action to process the unprotected status message and respond with a deregistration request suggests that it did not enforce the expected security policy of ignoring or discarding unprotected messages after security activation. This behavior could expose the UE to security risks, such as NAS message replay or injection attacks, and does not align with the 3GPP security requirements for NAS message protection post-authentication. Therefore, the UE's action in this scenario is considered insecure. Insecure
261	261	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0101 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.7511579990386963 UE to AMF UplinkNASTransport, Service request 0.7514059543609619 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE initiated a service request by sending an UplinkNASTransport message to the AMF. In response, the AMF sent a Security Mode Command message, which was protected (i.e., integrity protected and/or ciphered) using the negotiated security algorithms (128-5G-EA1 for ciphering and 128-5G-IA2 for integrity protection), and included the ABBA parameter. However, the UE did not respond to the Security Mode Command. According to the 3GPP 5G standard, after 5G-AKA, the UE and AMF must establish NAS security by exchanging and accepting the Security Mode Command and its response. The Security Mode Command is sent protected only after authentication, and the UE is expected to verify the message, apply the security context, and respond with a Security Mode Complete message. The lack of response from the UE means it did not acknowledge or accept the security context, which is a deviation from the standard procedure. This could indicate a security issue, such as the UE not accepting a properly protected message, or a failure to process the security context, potentially leaving the communication in an insecure or undefined state. Therefore, based on the 3GPP standard, the UE's action in not responding to a protected Security Mode Command after successful authentication is considered insecure. Insecure

262	262	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 8.914944887161255 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 8.915573835372925 AMF to UE SACK (Ack=13, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a Service Request to the AMF, which is a standard step to initiate or resume a session. The AMF then responded with a Security Mode Command, but crucially, this command was sent as a plain (unencrypted and unauthenticated) NAS message, with the ciphering algorithm set to 5G-EA0 (null ciphering) and the integrity algorithm set to 128-5G-IA2. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages—especially those that establish security contexts, such as the Security Mode Command—should be integrity protected and, where applicable, ciphered. The UE, upon receiving a Security Mode Command in plain text after authentication, is expected to reject or ignore such a message, as accepting it could expose the UE to security risks such as man-in-the-middle attacks or replay attacks. In this test, the UE did not respond to the plain Security Mode Command, which aligns with the security requirements of the 3GPP standard, as it did not accept or process a potentially insecure message. Therefore, the UE's action was secure. Secure
263	263	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 74 UE provided: No response The packet capture during the test using wireshark is: 0.5198588371276855 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5200669765472412 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Registration reject (Temporarily not authorized for this SNPN) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent an Uplink NAS Transport message (specifically, a PDU session establishment request) to the AMF. In response, the AMF sent a Registration Reject message with 5GMM Cause 74 ("Temporarily not authorized for this SNPN"), and this message was sent in plain (unencrypted) form. The UE, upon receiving this plain Registration Reject, did not respond further. According to the 3GPP 5G standard (TS 24.501), after 5G-AKA is completed, NAS security (encryption and integrity protection) should be activated for subsequent NAS messages, except for certain allowed exceptions (such as specific reject messages under defined conditions). However, the standard also specifies that if the UE receives a Registration Reject message in plain NAS after security has been established, it should not respond to it, as this could be a security attack (e.g., a downgrade or spoofing attempt). In this test, the UE correctly did not respond to the plain Registration Reject message after 5G-AKA was completed, demonstrating compliance with the 3GPP security requirements and protecting itself from potential attacks. Therefore, the UE's action was secure. Secure

264	264	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 6 UE provided: No response The packet capture during the test using wireshark is: 2.427165985107422 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4275641441345215 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4278719425201416 AMF to UE DownlinkNASTransport, Registration reject (Illegal ME) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the UE continues with NAS signaling. 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 standard (TS 24.501), after 5G-AKA is completed, NAS messages between the UE and the AMF should be integrity protected and, where possible, encrypted to ensure confidentiality and authenticity. However, the standard also specifies that certain messages, such as Registration Reject with specific causes (including "Illegal ME"), may be sent in plain text, as the UE may not be allowed to establish security contexts in these cases. The UE, upon receiving a plain Registration Reject with cause 6, is expected to not respond further, as it is not permitted to continue registration or communication. In this test, the UE did not respond to the plain Registration Reject, which aligns with the 3GPP specification and is considered a secure and compliant behavior, as the UE did not attempt to process or respond to an unprotected message beyond what is allowed by the standard. Secure

265	265_F	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1111 RAND: 0e38a634245d3e4aea72a7f7a7148161 AUTN: 3d9033e57f3e8000d3eb278394dd7c46 ngKSI_TSC: Native security context ngKSI_KSI: 5 UE provided: Authentication failure (ngKSI already in use) The packet capture during the test using wireshark is: 1.0084679126739502 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.0087080001831055 AMF to UE SACK (Ack=10, Arwnd=106496) , DownlinkNASTransport, Authentication request 1.216444969177246 UE to AMF UplinkNASTransport, Authentication failure (ngKSI already in use) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a service request to the AMF. The AMF, under test control, responded with an Authentication Request message sent in plain (unencrypted) NAS, even though a native security context had already been established (as indicated by ngKSI_TSC: Native security context and ngKSI_KSI: 5). Upon receiving this message, the UE replied with an Authentication Failure, specifically stating "ngKSI already in use." According to the 3GPP 5G security standards, once 5G-AKA is completed and a native 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 expected to reject or not process any further authentication requests for the same security context, especially if they are sent in plain text, as this could indicate a replay or downgrade attack. By refusing to process the plain, redundant authentication request and responding with an appropriate error, the UE adhered to the security requirements of the 5G standard, thereby protecting itself from potential security threats such as replay or man-in-the-middle attacks. Therefore, the UE's action was secure and compliant with 3GPP specifications. 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 to the UE, and this message was sent in plain (unencrypted) form. According to the 3GPP 5G standards, after the completion of 5G-AKA, both the UE and the AMF should have established NAS security (encryption and integrity protection) before exchanging further NAS messages, except for a few specific message types (such as Service Request or Deregistration Request under certain conditions). The Authentication Reject message, however, is one of the few messages that, per 3GPP TS 24.501, is allowed to be sent in plain NAS if the security context is not established or if the authentication procedure fails. In this case, since the 5G-AKA was completed, the expectation is that the UE should only accept an Authentication Reject if it is protected by NAS security. The UE, upon receiving a plain (unencrypted) Authentication Reject after 5G-AKA, did not respond, which aligns with the security requirements: the UE should ignore unprotected messages that require security after authentication is complete. This behavior prevents potential security attacks such as downgrading or spoofing. Therefore, the UE's action of not responding to the unprotected Authentication Reject message after 5G-AKA is considered secure and compliant with the 3GPP 5G standard. Secure

267	267	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.5199449062347412 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5201799869537354 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent an Uplink NAS Transport message to the AMF, which is expected behavior as the UE proceeds with further NAS signaling (such as a PDU session establishment request). The AMF, under test control, responded with an Authentication Reject message sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), after the completion of 5G-AKA, all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, where applicable, ciphered. The Authentication Reject message is an exception to this rule: per 3GPP TS 24.501, section 9.11.3.3, the AMF may send an Authentication Reject message in plain NAS, and the UE is required to silently discard it and not respond. In this test, the UE did not respond to the plain Authentication Reject message, which is the correct and secure behavior as specified by the standard. This prevents potential security attacks where an attacker could inject a plain Authentication Reject to disrupt service. Therefore, the UE's action in this scenario was secure and compliant with 3GPP requirements. Secure
268	268	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.7500498294830322 UE to AMF UplinkNASTransport, Registration complete 0.7504808902740479 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context should have been established. Subsequently, the AMF sent a "Configuration Update Command" to the UE, which was marked as "Protected," but the security header was reported as "Unknown," and the UE did not respond to this message. According to the 3GPP 5G standard, after 5G-AKA is completed, all subsequent NAS messages between the UE and the AMF must be integrity protected and, where required, encrypted using the established NAS security context. If the security header of the downlink message is not recognized or does not conform to the expected security context, the UE is expected to discard the message and not respond, as a security measure to prevent potential attacks or protocol violations. In this case, the UE's lack of response to a message with an unknown security header demonstrates adherence to the 3GPP security requirements, as it avoids processing potentially insecure or malformed messages. Therefore, the UE's action in this scenario was secure. Secure

269	269	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.46799302101135254 UE to AMF UplinkNASTransport, Registration complete 0.4681861400604248 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the NAS security context should have been established and that subsequent NAS messages should be protected (i.e., integrity protected and ciphered) as per 3GPP TS 24.501. However, the AMF then sent a "Deregistration Accept" message to the UE in plain (unencrypted and non-integrity protected) form, which is a deviation from the expected behavior after security activation. The UE, upon receiving this unprotected message, did not respond. According to the 3GPP standard, after security mode is activated, the UE must ignore any NAS messages that are not integrity protected and ciphered, except for a few specific cases (such as initial registration or service requests before security activation). By not responding to the unprotected "Deregistration Accept" message, the UE correctly adhered to the 3GPP security requirements, thereby preventing potential security risks such as replay or spoofing attacks. This behavior demonstrates that the UE's actions were secure and compliant with the 5G standard. Secure
270	270	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03999805450439453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04024100303649902 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an identity response to the AMF, and the AMF subsequently issued another identity request, specifically requesting the IMEISV, in plain (unencrypted) NAS signaling. At this point, the 5G-AKA authentication and key agreement procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to 3GPP standards (TS 24.501), sensitive information such as the IMEISV should not be transmitted in plain text before NAS security is activated, as this could expose the UE to privacy and security risks (e.g., IMEISV catching or tracking). The UE, in this case, did not respond to the AMF's plain (unencrypted) request for the IMEISV, which aligns with the security recommendations of the 3GPP standard to protect the subscriber's privacy and device identity. By refusing to send the IMEISV in the clear, the UE demonstrated secure behavior, as it did not disclose sensitive information before the establishment of a secure channel. Secure

271	271	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.03961491584777832 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.03991198539733887 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, and subsequently, the AMF sent another Identity Request asking for the IMEI, 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. According to the 3GPP 5G standard (TS 24.501), the UE is required to protect sensitive information such as the IMEI and SUPI by only transmitting them in plain text if NAS security has not been activated, and only when strictly necessary (e.g., initial registration). However, the standard also allows the UE to refuse to send the IMEI in response to a plain (unencrypted) Identity Request after the initial identity exchange, especially if the request appears suspicious or redundant. In this test, the UE did not respond to the AMF's plain Identity Request for the IMEI after already having sent an Identity Response, and before NAS security was established. This behavior aligns with the security recommendations of the 3GPP standard, as it prevents the unnecessary exposure of the IMEI in unprotected messages, thereby reducing the risk of IMEI interception or misuse. Therefore, the UE's action in refusing to respond to the unprotected Identity Request was secure and in accordance with 3GPP security guidelines. Secure
272	272	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007159709930419922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept 0.2011561393737793 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a Service Accept message, which was sent as a protected (encrypted or integrity-protected) NAS message. However, the 5G-AKA authentication procedure, which is required to establish NAS security (encryption and integrity protection), was not completed prior to this exchange. Despite this, the UE proceeded to send a Deregistration Request (UE originating) in uplink, responding to the Service Accept. According to the 3GPP 5G standard, NAS security (encryption and integrity protection) must be established via successful completion of 5G-AKA before any protected NAS messages are exchanged. The UE should not accept or process protected NAS messages from the network before security context is established, nor should it send further NAS messages in response to such protected messages. By responding to a protected Service Accept message before 5G-AKA completion, the UE failed to adhere to the required security procedures, potentially exposing itself to security risks such as replay or spoofing attacks. Therefore, the UE's action in this scenario was not secure according to 3GPP standards. Insecure

273	273	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.11984086036682129 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12007284164428711 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the UE sent an authentication response to the AMF, the AMF immediately sent a deregistration request to the UE. Notably, the 5G-AKA (Authentication and Key Agreement) procedure had not yet been completed, meaning that the security context for NAS message protection (integrity and ciphering) was not yet established. Despite this, the AMF sent the deregistration request as a protected message (integrity protected and ciphered), which the UE did not respond to. According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) must only be applied after successful completion of the 5G-AKA procedure, when both the UE and the network have established a shared security context. If the UE receives a protected NAS message before 5G-AKA is completed, it should ignore or discard the message, as it cannot verify or decrypt it without the necessary keys. The UE's lack of response to the protected deregistration request indicates that it correctly followed the 3GPP security procedures by not processing a protected message before security context establishment. Therefore, the UE's action was secure and compliant with the 5G standard. Secure
274	274	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.11959981918334961 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1198418140411377 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE completed the initial NAS steps and sent an authentication response to the AMF, but the 5G-AKA procedure was not yet completed, meaning that the NAS security context (encryption and integrity protection keys) had not been established. Immediately after receiving the authentication response, the AMF sent a deregistration request to the UE, which was marked as "integrity protected" in the security header. According to the 3GPP 5G standard, NAS message protection (integrity and encryption) should only be applied after successful completion of the 5G-AKA procedure, when both the UE and the AMF have derived the necessary security keys. Since the 5G-AKA was not completed, the UE would not have the required keys to verify or decrypt a protected message. The UE did not respond to the deregistration request, which is the correct and secure behavior as per the standard, because processing a protected message without the proper 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 deregistration request before 5G-AKA completion 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 initial 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 security keys for NAS message protection had not occurred. Despite this, the AMF responded with a deregistration request message that was integrity protected and ciphered, indicating that it was sent as a "protected" NAS message. According to the 3GPP 5G standard, the UE should only accept and process protected NAS messages after the successful completion of the 5G-AKA procedure, as this is when the necessary security context is established. Since the UE did not respond to the protected deregistration request (which was sent before security activation), it correctly adhered to the 3GPP security requirements by refusing to process a protected message before security context establishment. This behavior prevents potential security vulnerabilities, such as replay or spoofing attacks, that could arise if the UE accepted protected messages without proper authentication and key agreement. Therefore, the UE's action in this scenario was secure. Secure
276	276	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3232 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 1.6001770496368408 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Identity response 1.6007089614868164 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF engaged in NAS communication where, after the UE sent an identity response, the AMF issued a Security Mode Command as a plain (unencrypted) NAS message. Notably, the 5G-AKA authentication procedure had not yet been completed, which is a prerequisite for establishing NAS security (encryption and integrity protection) as per 3GPP standards. The Security Mode Command from the AMF specified ciphering and integrity algorithms, but since it was sent in plain text and the 5G-AKA was not completed, the UE did not have the necessary security context to process this command securely. The UE responded by not replying to the Security Mode Command. According to 3GPP TS 24.501, the UE must not accept or process security mode commands before the completion of authentication and establishment of a security context, as this could expose the UE to security risks such as downgrade or man-in-the-middle attacks. By refusing to respond to the Security Mode Command sent in plain text before authentication, the UE adhered to the security requirements of the 5G standard and protected itself from potential vulnerabilities. Secure

277	277	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.04006814956665039 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040535926818847656 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE and AMF were engaged in NAS communication as part of the 5G registration process. The UE sent an Identity Response message to the AMF, which is a normal step before authentication. However, before the 5G-AKA (Authentication and Key Agreement) procedure was completed, the AMF sent a Configuration Update Command to the UE. Notably, this downlink message from the AMF was sent with integrity protection enabled, but since the 5G-AKA had not yet been completed, the necessary NAS security context (keys for integrity and encryption) had not been established. According to the 3GPP 5G standard (TS 24.501), NAS security procedures (integrity and encryption) must only be applied after successful authentication and security mode command exchange, which establishes the required keys. The UE, upon receiving a protected message before security context establishment, is expected to ignore or reject such messages, as processing them could expose it to security risks such as replay or impersonation attacks. In this test, the UE did not respond to the prematurely protected Configuration Update Command, which aligns with the 3GPP security requirements and demonstrates correct, secure behavior. The UE's refusal to process or respond to a protected message before security activation ensures that it is not vulnerable to protocol misuse or attacks at this stage of the registration process. Secure
278	278	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.3110721111297607 UE to AMF UplinkNASTransport, Identity response 2.311551094055176 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Configuration update command 2.3115811347961426 UE to AMF SACK (Ack=3, Arwnd=106437) , UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, which is expected to be sent in plain NAS as the 5G-AKA authentication and key agreement had not yet been completed. The AMF then sent a Configuration Update Command to the UE, also in plain NAS, which is not standard practice according to 3GPP specifications. Configuration Update Command is a security-protected message and should only be sent after the NAS security context is established (i.e., after 5G-AKA is completed and NAS security mode is activated). The UE, upon receiving this unprotected Configuration Update Command before security activation, did not process the message and instead initiated a Deregistration Request, effectively refusing to act on the insecure command. This behavior aligns with 3GPP security requirements, which state that the UE must not accept or process security-sensitive NAS messages in plain text after the initial registration steps, and should deregister or ignore such messages to prevent potential security breaches. Therefore, the UE's action demonstrates correct and secure behavior as per the 5G standard. Secure

279	279	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007669925689697266 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. However, before the 5G-AKA authentication and key agreement procedure was completed—which is required to establish security context and enable encryption and integrity protection for NAS messages—the AMF responded with a deregistration accept message. Notably, this downlink message from the AMF was sent as "protected," even though the security context had not yet been established. The UE, upon receiving this 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 a protected NAS message is received before security context establishment, the UE is expected to discard it and not respond, as it cannot verify or decrypt the message. The UE's lack of response in this scenario aligns with the 3GPP security requirements, as it did not process or acknowledge a protected message sent prematurely. Therefore, the UE's behavior was secure and compliant with the 5G standard. Secure
280	280	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007870197296142578 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. However, before the 5G-AKA authentication and key agreement procedure was completed—which is required to establish security context and enable encryption and integrity protection for NAS messages—the AMF responded with a deregistration accept message that was protected (i.e., integrity protected and/or encrypted). According to the 3GPP 5G standard, the UE should only process protected NAS messages after a security context has been established via 5G-AKA. Since the 5G-AKA was not completed, the UE had no valid security context and therefore could not verify or decrypt the protected deregistration accept message. The UE correctly did not respond to this message, as processing or responding to protected messages without a valid security context would be a security vulnerability. This behavior aligns with the 3GPP standard, which mandates that UEs must ignore protected NAS messages if security has not been activated. 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 test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a configuration update command that was integrity protected and ciphered using a new security context, as indicated by the security header type (4). However, the 5G-AKA (Authentication and Key Agreement) procedure, which is responsible for establishing the security context and keys for NAS message protection, had not yet been completed at the time the AMF sent the protected configuration update command. 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 the security context is not valid until then. The UE, upon receiving a protected NAS message before security context establishment, is expected to discard the message and not respond, as processing such a message would be insecure and non-compliant with the standard. In this test, the UE did not respond to the prematurely protected configuration update command, which aligns with the 3GPP security requirements and demonstrates correct, secure behavior. Secure
282	282	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006248950958251953 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, before the completion of the 5G-AKA authentication and key agreement procedure, responded with a configuration update command that was integrity protected and ciphered (i.e., sent as a "protected" NAS message). According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) can only be applied after the successful completion of the 5G-AKA procedure, which establishes the necessary security context and keys between the UE and the network. Since the 5G-AKA was not completed at the time the AMF sent the protected message, the UE, adhering to the standard, did not respond to the configuration update command. This is the correct and secure behavior, as processing or responding to protected NAS messages before security context establishment 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 in line with 3GPP security requirements and demonstrates secure behavior. Secure

283	283	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006029605865478516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an InitialUEMessage containing a Registration Request to the AMF. The AMF, under test control, responded with a DownlinkNASTransport message carrying a Service Accept, which was sent as a protected (i.e., integrity protected and/or encrypted) NAS message. However, the 5G-AKA authentication and key agreement procedure had not yet been completed at this point in the exchange, meaning that the necessary security context for NAS message protection (encryption and integrity protection) had not been established between the UE and the network. According to the 3GPP 5G standard, specifically TS 24.501, the UE should only accept protected NAS messages after the security context is established via 5G-AKA. Since the UE did not respond to the protected Service Accept message sent before security activation, it correctly rejected or ignored the message, adhering to the standard and preventing a potential security vulnerability where an attacker could send protected messages before authentication. Therefore, the UE's action was secure and compliant with 3GPP requirements. 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 message containing a Service Accept, which was sent as a protected (i.e., integrity protected and/or encrypted) message. However, the 5G-AKA authentication procedure, which is required to establish NAS security (encryption and integrity protection of NAS messages), was not completed prior to this exchange. According to the 3GPP 5G standard, the Service Accept message should only be sent after successful completion of 5G-AKA and establishment of NAS security context. The UE, upon receiving a protected Service Accept message before security context was established, responded by sending a Deregistration Request, effectively aborting the registration process. This behavior aligns with 3GPP security requirements, as the UE should not accept or process protected NAS messages before security activation, and should terminate the procedure if protocol violations are detected. Therefore, the UE's action demonstrates correct and secure handling of the protocol, as it did not proceed with an insecure or out-of-spec communication. Secure

285	285	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.039772987365722656 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (PLMN not allowed) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response message to the AMF, which is expected behavior when the network requests the UE's identity. However, immediately after this, the AMF sent a Deregistration Request message to the UE, which was integrity protected and ciphered (security header type 2). According to the 3GPP 5G standard, NAS message protection (integrity and ciphering) can only be applied after the 5G-AKA authentication and key agreement procedure is successfully completed, as this is when the necessary security context is established between the UE and the network. In this case, the 5G-AKA procedure had not yet been completed, so the UE had not established the required NAS security context. The UE did not respond to the protected Deregistration Request message from the AMF. This behavior is correct and secure according to the 3GPP standard, as the UE should ignore or discard any NAS messages that are protected (integrity protected and/or ciphered) before the security context is established. Responding to such a message could indicate a security flaw, as it would mean the UE is processing messages that it cannot verify or decrypt securely. Therefore, the UE's action of not responding to the protected Deregistration Request before 5G-AKA completion is in line with 3GPP security requirements and demonstrates secure behavior. Secure
286	286	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00036406517028808594 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. The AMF, under test control, responded with a protected (i.e., integrity protected and/or encrypted) GMM status message with cause 98 ("Message type not compatible with the protocol state"). According to 3GPP standards (TS 24.501), before NAS security is established, the UE should only process unprotected NAS messages; any protected NAS message received before the completion of 5G-AKA should be ignored or discarded by the UE. In this test, the UE did not respond to the protected GMM status message sent by the AMF prior to security establishment, which aligns with the expected secure behavior as per the 3GPP standard. This indicates that the UE correctly ignored a message that should not be processed before security activation, thereby preventing potential security vulnerabilities such as replay or spoofing attacks. Secure

287	287	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 3 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.000408172607421875 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Illegal UE) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a 5G standalone registration by sending an initial registration request to the AMF. The AMF, under test control, responded with a GMM status message indicating a 5GMM cause of 3 ("Illegal UE"), and this message was sent as "protected" (i.e., integrity protected and/or encrypted). However, the 5G-AKA authentication procedure had not yet been completed, meaning that the necessary security context for NAS message protection (encryption and integrity protection) was not yet established between the UE and the AMF. According to the 3GPP 5G standard, the UE should not accept or process protected NAS messages before the completion of 5G-AKA, as the keys required for protection are not yet available. The UE, in this case, did not respond to the protected GMM status message from the AMF, which is the correct and secure behavior as per the standard. This prevents potential security vulnerabilities such as replay or spoofing attacks before mutual authentication and key establishment. Therefore, the UE's action of not responding to a protected NAS message before 5G-AKA completion aligns with 3GPP security requirements and demonstrates secure behavior. Secure
288	288	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0008118152618408203 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.20334196090698242 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the UE initiated a registration procedure by sending an initial registration request to the AMF. The AMF responded with a Security Mode Command, which was protected using integrity protection (128-5G-IA2) but did not use ciphering (5G-EA0, the null cipher algorithm), and indicated a new security context. Importantly, the 5G-AKA authentication procedure had not yet been completed, meaning that the mutual authentication and key agreement necessary for establishing secure NAS encryption had not taken place. Upon receiving the Security Mode Command, the UE responded with a 5GMM status message indicating "Invalid mandatory information." According to the 3GPP 5G standard, the UE should not accept a Security Mode Command that is protected with a new security context before the 5G-AKA procedure is completed, as the necessary keys for secure communication have not yet been established. By rejecting the Security Mode Command and indicating invalid mandatory information, the UE correctly refused to proceed with security procedures that would have been insecure, as the cryptographic context was not yet valid. This behavior aligns with the security requirements of the 5G standard, as it prevents the establishment of a security context without proper authentication and key agreement. Therefore, the UE's action in this scenario was secure. Secure

289	289	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 6.12048602104187 UE to AMF SACK (Ack=5, Arwnd=106496) , UplinkNASTransport, Identity response 6.120656967163086 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, and subsequently, the AMF sent another Identity Request, specifically requesting the GUTI, in plain (unencrypted) NAS signaling. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard (TS 24.501), the UE is required to be cautious about sending sensitive information, such as the GUTI, over unprotected NAS messages. If the AMF requests the GUTI in plain NAS before security is activated, the UE should not respond with the requested identity to avoid exposing potentially sensitive information. In this test, the UE did not respond to the AMF's plain Identity Request for the GUTI, which aligns with the security requirements of the 5G standard to protect user privacy and prevent identity exposure before security activation. Therefore, the UE's action was secure and compliant with 3GPP guidelines. 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 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 in plain text over the air interface; instead, it should only be sent after a secure NAS security context has been established, which occurs after successful completion of 5G-AKA. In this case, the UE did not respond to the AMF's plain (unencrypted) identity request for the IMEISV, which aligns with the security requirements to protect the subscriber's privacy and device identity. By refusing to send the IMEISV in the clear, the UE demonstrated correct and secure behavior as per 3GPP standards, ensuring that sensitive information is not exposed before encryption is in place. Secure

291	291	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.03981208801269531 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04005002975463867 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the initial NAS procedures, the UE sent an Identity Response to the AMF, and the AMF subsequently sent another Identity Request, specifically requesting the TMSI, in plain (unencrypted) NAS message format. At this point, the 5G-AKA authentication procedure had not yet been completed, meaning that NAS security (encryption and integrity protection) was not yet established. According to the 3GPP 5G standard (TS 24.501), the UE is required to respond to identity requests even if NAS security is not yet activated, but there are important security considerations: if the AMF requests a sensitive identifier (such as the SUPI or IMSI) in plain text, the UE should avoid sending it in the clear and may either refuse to respond or send a less sensitive identifier (like the TMSI or GUTI) if available. In this test, the AMF requested the TMSI in plain text, and the UE did not respond. This behavior aligns with a security-conscious implementation, as the UE avoided exposing its TMSI in an unprotected message, which could otherwise be vulnerable to interception or replay attacks. By withholding its response until NAS security is established, the UE demonstrates adherence to the principle of minimizing exposure of sensitive information before a secure channel is in place. Therefore, the UE's action in this scenario is consistent with secure behavior as recommended by the 3GPP standard. 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) (RES accepted) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the 5G standalone User Equipment (UE) completed the initial NAS steps and sent an authentication response to the Access and Mobility Management Function (AMF), but the 5G-AKA (Authentication and Key Agreement) procedure was not yet completed. Immediately after receiving the authentication response, the AMF sent a deregistration request to the UE, which was integrity protected but not encrypted, as encryption is only 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 only accept and process protected NAS messages (such as deregistration requests) after the security context is established, which occurs upon successful completion of 5G-AKA. Since the 5G-AKA was not completed, the UE correctly did not respond to the deregistration request, as it could not verify the authenticity and integrity of the message without the established security context. This behavior aligns with the 3GPP security requirements, as it prevents potential security breaches such as replay or spoofing attacks before mutual authentication and key agreement are finalized. 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 test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "Registration Complete" message to the AMF, indicating that the initial NAS security context should have been established and all subsequent NAS messages should be protected (i.e., integrity protected and ciphered) as per 3GPP TS 24.501. However, the AMF then sent a "Configuration Update Command" as a plain (unencrypted and non-integrity protected) NAS message, which is not compliant with the 5G security requirements post-authentication. The UE, upon receiving this plain NAS message after security context establishment, did not respond. According to 3GPP standards, the UE is required to discard any plain NAS messages received after security activation and not respond to them, as accepting or processing such messages could expose the UE to security risks such as replay or man-in-the-middle attacks. Therefore, the UE's action of not responding to the plain "Configuration Update Command" was correct and in line with 3GPP security requirements, demonstrating secure behavior in this context. Secure
294	294	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3030 RAND: 313131313131313131005fb686550000 AUTN: 3030303030303000ee555fb686550000 ngKSI_TSC: Mapped security context ngKSI_KSI: 2 UE provided: No response The packet capture during the test using wireshark is: 0.11998605728149414 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.12024092674255371 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated security algorithms and was ready to begin protected NAS communication. However, the AMF then sent an "authentication request" message to the UE in plain (unencrypted) form, despite the fact that, according to the 3GPP 5G standard, all subsequent NAS messages after the security mode complete should be integrity protected and, if possible, encrypted. The UE, upon receiving this unexpected and insecure plain authentication request after security activation, did not respond. This behavior aligns with the 3GPP security requirements, which state that the UE must not process or respond to NAS messages that are not properly protected after security has been activated. By refusing to respond to an unprotected message after security mode completion, the UE demonstrated secure behavior and adherence to the 5G standard, thereby preventing potential security vulnerabilities such as replay or downgrade attacks. Secure

295	295	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.16016411781311035 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16040301322937012 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of 5G-AKA authentication, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to begin secure NAS communication. However, the AMF responded with a "service reject" message, which was sent in plain (unencrypted) form and included a 5GMM cause code 111 (Protocol error, unspecified). According to the 3GPP 5G standard (TS 24.501), once the security context is established (i.e., after 5G-AKA and security mode complete), all subsequent NAS messages between the UE and the AMF must be integrity protected and, if required, ciphered. The UE, upon receiving a plain (unencrypted and unprotected) NAS message after security activation, should ignore such messages and not process them, as processing unprotected messages after security activation could expose the UE to security risks such as replay or downgrade attacks. In this test, the UE did not respond to the unprotected "service reject" message, which is the correct and secure behavior as per the 3GPP standard. By refusing to process or respond to a plain NAS message after security activation, the UE demonstrated compliance with the security requirements of 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 begin secure NAS communication. However, the AMF subsequently sent an "authentication request" message to the UE in plain (unencrypted) form, even though the security context should have already been established. According to the 3GPP 5G standard, once the security mode is complete, all subsequent NAS messages between the UE and the AMF must be integrity protected and, if required, encrypted. The UE, upon receiving a plain (unencrypted) authentication request after security mode completion, did not respond. This behavior aligns with the 3GPP standard, as the UE is expected to reject or ignore any NAS messages that are not properly protected after security activation. By not responding to the insecure message, the UE demonstrated correct and secure behavior, ensuring that sensitive information is not exposed and that the integrity of the communication is maintained. Secure

297	297	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.16003108024597168 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16027402877807617 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the negotiated NAS security algorithms and was ready to communicate securely. Immediately after, the AMF sent a "deregistration accept" message to the UE, but this message was sent in plain (unencrypted) NAS, as observed in the packet capture. According to the 3GPP 5G standard (TS 24.501), once NAS security is activated (i.e., after the security mode complete message), all subsequent NAS messages exchanged between the UE and the AMF must be integrity protected and, if required, ciphered. The fact that the UE did not respond to the plain "deregistration accept" message from the AMF demonstrates that the UE correctly enforced the 5G security requirements by refusing to process a downlink NAS message that was not protected after security activation. This behavior aligns with the 3GPP standard, as the UE must ignore any unprotected NAS messages after security mode is established. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure
298	298	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.1601550579071045 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16047000885009766 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, after the successful completion of the 5G-AKA authentication procedure, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to begin secure NAS communication. However, the AMF then sent an "authentication reject" message to the UE, and notably, this message was sent in plain (unencrypted) form. According to the 3GPP 5G standard (TS 24.501), once the security context is established (i.e., after 5G-AKA and security mode complete), all subsequent NAS messages between the UE and the AMF must be integrity protected and, where applicable, encrypted. The "authentication reject" message, if sent after security mode complete, should be protected; otherwise, it could be exploited by an attacker to trigger denial-of-service or downgrade attacks. In this test, the UE did not respond to the unprotected "authentication reject" message, which aligns with the 3GPP security requirements: the UE must ignore any NAS messages that are not integrity protected after security mode is established. This behavior prevents potential security breaches and ensures the integrity of the communication. Therefore, the UE's action in this scenario was secure and compliant with the 5G standard. Secure

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