UE Response Evaluation Report: Test time: 2025-07-21 18:02:49

SL	Test Name	Test content	Remark
1	1	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006918907165527344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. Following this, the AMF responded with an identity request, specifically asking for the International Mobile Equipment Identity (IMEI) of the UE. Notably, this identity request was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The UE did not provide a response to the identity request. According to the 3GPP standards, the 5G-AKA procedure must be completed before any NAS messages can be encrypted, ensuring the confidentiality and integrity of the communication. By not responding to the identity request sent in plain text, the UE avoided exposing its IMEI, which is a sensitive identifier. This action aligns with the security principles of minimizing the exposure of sensitive information, especially when the communication is not yet secured through encryption. Therefore, the UE's decision to withhold its IMEI in this context can be considered a secure action, as it prevents potential interception of sensitive data before the establishment of a secure communication channel. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. Following this, the AMF, which was under test control, sent an identity request to the UE. Notably, this identity request was transmitted in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The AMF requested the Subscription Concealed Identifier (SUCI) from the UE, and the UE responded with an identity response. According to the 3GPP standards, the 5G-AKA procedure must be completed before any NAS messages can be encrypted, ensuring the confidentiality and integrity of the communication. Since the 5G-AKA was not completed, the UE's response to the identity request was sent without encryption, exposing sensitive information like the SUCI to potential interception. This lack of encryption before the completion of the 5G-AKA process indicates a security vulnerability, as the UE should ideally not transmit sensitive identity information in plain text. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario was insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was initiated by the UE sending an initial registration request. This uplink message was followed by a downlink message from the AMF, which was an authentication reject sent in plain text. The UE did not provide any response to this message. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to establish a secure communication channel, ensuring that subsequent messages are encrypted. In this scenario, the 5G-AKA was not completed, and the AMF's message was sent in plain text, which is a potential security risk as it could be intercepted or tampered with by malicious entities. The UE's lack of response to the authentication reject could be seen as a cautious approach, as it did not proceed with any further actions that could compromise its security. However, the fact that the UE did not engage in any further communication or attempt to reinitiate the authentication process leaves it in a state of uncertainty regarding its security posture. Based on the 3GPP standards, the UE's action of not responding to an unencrypted authentication reject message can be considered a secure approach, as it avoids engaging in potentially insecure communication. Therefore, the UE's behavior in this test scenario can be deemed "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 User Equipment (UE) initiated communication with the Access and Mobility Management Function (AMF) by sending an initial registration request. In response, the AMF sent an identity request to the UE, requesting the Subscription Concealed Identifier (SUCI). The UE then provided an identity response. Notably, the identity request from the AMF was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. According to the 3GPP standards, the 5G-AKA procedure is essential for establishing a secure communication channel, as it ensures that messages are encrypted and protected from interception. Since the 5G-AKA was not completed, the communication between the UE and AMF, particularly the identity request and response, was not encrypted. This lack of encryption means that sensitive information, such as the SUCI, could potentially be exposed to unauthorized parties. Therefore, based on the 3GPP standards, the action taken by the UE in responding to an unencrypted identity request is considered insecure, as it does not adhere to the security protocols designed to protect user identity and data. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. The AMF responded with a registration reject message, citing a protocol error with an unspecified cause (5GMM Cause: 111). Notably, this downlink message from the AMF was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is a prerequisite for encrypting NAS messages. Following the registration reject, the UE sent a deregistration request, indicating its decision to terminate the registration process. The UE's actions in this scenario were in line with the 3GPP standards, as it appropriately responded to the registration reject by initiating deregistration. However, the fact that the initial registration request and subsequent deregistration request were sent without encryption due to the incomplete 5G-AKA process raises concerns about the security of the communication. The lack of encryption means that sensitive information could potentially be exposed to unauthorized parties. Therefore, while the UE's procedural response was correct, the communication itself was insecure due to the absence of encryption. Insecure
6	6	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 22 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0009021759033203125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Congestion) 0.20517516136169434 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. The AMF responded with a registration reject message, citing congestion as the cause (5GMM Cause: 22). Notably, this downlink message from the AMF was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is a prerequisite for encrypting NAS messages. Following the rejection, the UE sent a deregistration request, indicating that it originated the deregistration process. According to the 3GPP standards, the UE's actions can be considered insecure. The UE should ideally not proceed with sensitive operations or send deregistration requests in plain text without the completion of the 5G-AKA, as this leaves the communication vulnerable to interception and manipulation. The lack of encryption due to the incomplete 5G-AKA process exposes the UE to potential security threats, as the integrity and confidentiality of the messages are not protected. Therefore, the UE's communication in this scenario is deemed insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. The AMF responded with an authentication request, which was sent in plain text, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI, which are typically used to authenticate the UE and establish a secure communication context. However, the UE responded with an authentication failure message, specifically citing "Non-5G authentication unacceptable." This response suggests that the UE detected an issue with the authentication request, possibly due to the use of a non-5G compliant method or parameters, and therefore rejected the authentication attempt. According to the 3GPP standards, the UE is expected to ensure that any authentication procedure adheres to the 5G security protocols before proceeding. By rejecting the authentication request that did not meet the 5G standards, the UE demonstrated adherence to the security requirements, thereby preventing potential security vulnerabilities. Therefore, the action taken by the UE was in line with the 5G security standards, ensuring that only secure and compliant authentication processes are accepted. Secure

8	8	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 313030300000000078742b94d4550000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Native security context ngKSI_KSI: 7 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005857944488525391 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.20240378379821777 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. Following this, the AMF responded with an authentication request, which was sent in plain text. The authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI values. However, the UE responded with a 5GMM status indicating "Invalid mandatory information." This response suggests that the UE detected an issue with the received authentication request, possibly due to the AUTN being all zeros, which is not a valid value. According to the 3GPP standards, the 5G-AKA procedure must be completed to establish a secure context for encrypting messages. Since the 5G-AKA was not completed, the communication remained unencrypted, and the UE's response indicates it did not proceed with the authentication process due to the invalid information. This behavior aligns with the security protocols outlined by 3GPP, as the UE correctly identified and rejected an invalid authentication attempt, thereby preventing potential security breaches. Therefore, the action taken by the UE was secure. Secure

9	9	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03973102569580078 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04003596305847168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.24200010299682617 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the exchange of NAS messages. Initially, the UE sent an identity response to the AMF, which was followed by an identity request from the AMF. Notably, the identity request from the AMF was sent in plain text, and the requested identity from the UE was the Subscription Concealed Identifier (SUCI). The UE responded with an identity response. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed. However, in this test, the 5G-AKA was not completed, meaning that the communication was not encrypted. The UE's action of responding to an identity request sent in plain text without the completion of 5G-AKA indicates a potential security vulnerability. The UE should ideally not transmit sensitive information like SUCI in an unencrypted manner, as this could expose the identity of the subscriber to potential interception. Therefore, based on the 3GPP standards and the lack of encryption in this interaction, the action taken by the UE is considered insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an identity response. Subsequently, the AMF sent an authentication request to the UE. Notably, this authentication request was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is necessary for establishing a secure communication channel. The UE responded with an authentication failure message, indicating that the ngKSI (NAS key set identifier) was already in use. This response suggests that the UE detected a potential security issue, as the ngKSI is used to identify the security context, and reusing an ngKSI could lead to vulnerabilities such as replay attacks. According to the 3GPP standards, the UE's action to reject the authentication request due to the reuse of an ngKSI is a secure behavior, as it prevents the establishment of a potentially compromised security context. The UE's response aligns with the security protocols designed to protect against unauthorized access and ensure the integrity of the communication. Therefore, the UE's action in this scenario was secure. Secure
11	11	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 11 UE provided: No response The packet capture during the test using wireshark is: 0.039990901947021484 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04016995429992676 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Service reject (PLMN not allowed) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response message to the AMF. Following this, the AMF sent a service reject message back to the UE, indicating that the Public Land Mobile Network (PLMN) was not allowed, with a 5GMM Cause value of 11. Notably, the service reject message was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is a prerequisite for encrypting NAS messages. The UE did not provide any response to the service reject message. According to the 3GPP standards, the 5G-AKA procedure is essential for establishing a secure communication channel between the UE and the network, ensuring that messages are encrypted and protected from potential interception or tampering. Since the 5G-AKA was not completed, the communication remained unencrypted, leaving the UE's identity response potentially exposed. This lack of encryption before the completion of the 5G-AKA process indicates a vulnerability in the security of the UE's communication. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario was insecure. Insecure

12	12	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.03978896141052246 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04010796546936035 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request 0.2456059455871582 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the exchange of identity messages. Initially, the UE sent an identity response to the AMF, which was followed by the AMF sending an identity request back to the UE. Notably, the AMF's identity request was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The AMF requested the Subscription Concealed Identifier (SUCI) from the UE, and the UE responded with an identity response. According to the 3GPP standards, the SUCI is a privacy-preserving identifier that should be protected to prevent exposure of the subscriber's identity. However, since the 5G-AKA procedure was not completed, the communication was not encrypted, leaving the identity information vulnerable to interception. The UE's action of responding to an unencrypted identity request with potentially sensitive information, such as the SUCI, without the protection of encryption, does not align with the security expectations of the 5G standard. Therefore, the UE's action in this scenario can be considered insecure, as it exposes sensitive identity information without the necessary cryptographic protection. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an authentication reject message. The test indicates that the 5G Authentication and Key Agreement (5G-AKA) procedure was not completed, which is crucial for establishing a secure communication channel. The packet capture shows that the authentication reject message from the AMF was sent in plain text, which is expected since encryption of NAS messages is contingent upon the successful completion of the 5G-AKA process. The UE did not provide any response to the authentication reject message. According to the 3GPP standards, the UE should not proceed with any sensitive operations or communications until a secure channel is established through the completion of the 5G-AKA. The lack of response from the UE to the plain-text authentication reject message suggests that the UE did not proceed with any further actions that could compromise security. Therefore, based on the 3GPP standards, the UE's behavior in not responding to an unauthenticated and unencrypted message is considered secure, as it prevents potential exploitation or unauthorized access. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response message to the AMF. Following this, the AMF sent a registration reject message back to the UE, citing congestion as the cause (5GMM Cause: 22). Notably, the downlink message from the AMF was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed. According to the 3GPP standards, the 5G-AKA procedure is crucial for establishing a secure communication channel, as it ensures that messages are encrypted and protected from potential interception or tampering. Since the 5G-AKA was not completed, the communication between the UE and the AMF remained unencrypted, leaving it vulnerable to security threats. The UE's action of sending an identity response without the completion of 5G-AKA indicates a lack of secure communication, as it did not ensure that the messages were encrypted before transmission. Therefore, based on the 3GPP standards, the UE's communication in this scenario was insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an authentication request. The authentication request was sent in plain text, which is unusual as per the 5G standard, where messages should be encrypted after the 5G Authentication and Key Agreement (5G-AKA) procedure is completed. The AMF's authentication request included a RAND and AUTN, but the AUTN was all zeros, which is not a valid authentication token. The UE responded with an authentication failure message, indicating that the non-5G authentication was unacceptable. This response from the UE is consistent with the 3GPP standards, which require the UE to reject any authentication attempts that do not conform to the 5G-AKA procedure. The UE's action to reject the authentication request due to the invalid AUTN and the lack of encryption aligns with the security protocols outlined by 3GPP, ensuring that the UE does not proceed with an insecure authentication process. Therefore, the UE's response was appropriate and secure according to the 5G standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. Subsequently, the AMF sent a Security Mode Command to the UE. Notably, the Security Mode Command was sent as a plain NAS message, which means it was not encrypted. The UE, however, did not provide any response to this command. According to the 3GPP standards, after the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the Security Mode Command was sent in plain text indicates a potential vulnerability, as it exposes the message to interception and tampering. The UE's lack of response could be interpreted as a failure to proceed with the security mode setup, which is a critical step in establishing a secure communication channel. This lack of response might suggest that the UE detected the plain text message as a security risk and chose not to proceed, which would be a secure action. However, without further context on why the UE did not respond, it is difficult to definitively conclude the security posture. Based on the information provided, the UE's action of not responding to a plain text Security Mode Command aligns with secure behavior as per 3GPP standards, which emphasize the importance of encrypted communication post-authentication. Therefore, the UE's action can be considered "Secure."
17	17	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: No response The packet capture during the test using wireshark is: 0.35177087783813477 UE to AMF UplinkNASTransport, Authentication response 0.35199785232543945 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response to the AMF. Following this, the AMF sent a service reject message back to the UE, which was transmitted in plain text. The 5G-AKA (Authentication and Key Agreement) procedure was not completed, which is crucial for establishing a secure communication channel. The 5GMM Cause code 111 indicates a "Protocol error, unspecified," suggesting that the service reject was due to an undefined protocol issue. Since the 5G-AKA was not completed, the messages exchanged were not encrypted, leaving the communication vulnerable to interception and tampering. According to the 3GPP standards, the completion of the 5G-AKA is essential for ensuring that subsequent NAS messages are encrypted and secure. The UE's lack of response to the service reject message further indicates a potential issue in handling protocol errors securely. Given that the communication was not encrypted and the UE did not take any corrective action, the interaction can be considered insecure based on the 5G standard outlined by 3GPP. Therefore, the UE's actions in this scenario were "Insecure."

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 User Equipment (UE) engaged in a Non-Access Stratum (NAS) communication with the Access and Mobility Management Function (AMF) as part of a 5G standalone network security test. The UE sent an authentication response to the AMF, which is a standard step in the 5G Authentication and Key Agreement (5G-AKA) procedure. However, before the 5G-AKA process was completed, the AMF sent an identity request to the UE, requesting the Subscription Concealed Identifier (SUCI). Notably, this identity request was sent in plain text, as encryption of NAS messages is contingent upon the completion of the 5G-AKA process. The UE responded with an identity response, providing the requested SUCI. According to the 3GPP standards, the SUCI is a privacy-preserving identifier that should be protected to prevent exposure of the subscriber's identity. Since the 5G-AKA process was not completed, the communication was not encrypted, potentially exposing sensitive information. The UE's action of responding to an unencrypted identity request with its SUCI, without the protection of encryption, is considered insecure as it could lead to privacy breaches. Therefore, based on the 3GPP standards, the UE's action in this scenario was insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is essential for establishing a secure communication context. Following this, the UE sent an authentication response to the AMF, which then replied with a security mode command. This command was sent as a protected message, utilizing the 5G-EA0 (null) cipher algorithm and the 128-5G-IA2 integrity algorithm, with a security header indicating integrity protection with a new security context. However, the UE responded with a security mode reject message, citing an unspecified reason for rejection. The UE's decision to reject the security mode command could be considered secure based on the 3GPP standards if the UE detected any inconsistencies or potential security vulnerabilities in the security mode command, such as the use of the null cipher algorithm (5G-EA0), which does not provide encryption. The rejection suggests that the UE prioritized maintaining a secure communication channel by not accepting a potentially insecure configuration. Therefore, the UE's action aligns with the security principles of ensuring data integrity and confidentiality, as outlined by the 3GPP standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was focused on the authentication process. Initially, the UE sent an authentication response to the AMF, which was followed by the AMF sending an authentication request back to the UE. Notably, the downlink message from the AMF was sent in plain text, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, as encryption of messages is contingent upon the successful completion of this procedure. The UE then responded with another authentication response. According to the 3GPP standards, the 5G-AKA procedure is crucial for establishing a secure communication channel, as it ensures mutual authentication and the derivation of security keys for encrypting subsequent messages. The fact that the AMF sent the authentication request in plain text suggests that the security context was not established, and the UE's response to this plain text message without the completion of 5G-AKA indicates a potential vulnerability. The UE should ideally not proceed with sensitive exchanges until a secure context is confirmed. Therefore, based on the 3GPP standards, the action taken by the UE in responding to an unencrypted authentication request without a completed 5G-AKA process is considered insecure. Insecure

21	21	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 303030303030300078d431f251560000 AUTN: 4953cc15a85a90008f0a1f4e8f0a3310 ngKSI_TSC: Native security context ngKSI_KSI: 4 UE provided: Authentication failure (MAC failure) The packet capture during the test using wireshark is: 1.8795151710510254 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, Authentication response 1.8797390460968018 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication request 2.0836050510406494 UE to AMF UplinkNASTransport, Authentication failure (MAC failure) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was focused on the authentication process. Initially, the UE sent an authentication response to the AMF, which was followed by an authentication request from the AMF. Notably, the AMF sent this request as a plain message, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, as encryption of messages is contingent upon the successful completion of this procedure. The UE subsequently responded with an authentication failure message, citing a MAC (Message Authentication Code) failure. This response from the UE suggests that it detected an inconsistency or potential tampering with the authentication request, as the MAC is used to ensure the integrity and authenticity of the message. According to the 3GPP standards, the UE's action to reject the authentication request due to a MAC failure is a secure response, as it prevents the UE from proceeding with potentially compromised or unauthorized communication. By adhering to the standard security protocols and identifying a MAC failure, the UE demonstrated a secure handling of the situation, ensuring that it did not proceed with an insecure authentication process. 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: 31313131313131310057a1d8550000 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was focused on the authentication process. Initially, the UE sent an authentication response to the AMF, which was followed by an authentication request from the AMF. Notably, the AMF sent this request as a plain message, which is unusual because, according to the 3GPP standards, messages should be encrypted after the 5G Authentication and Key Agreement (5G-AKA) procedure is completed. The UE responded with an authentication failure message, indicating that the non-5G authentication was unacceptable. This response suggests that the UE correctly identified the anomaly in the authentication process, as the 5G-AKA was not completed, and the message was sent in plain text, which is not secure. The UE's action to reject the authentication request aligns with the 3GPP standards, which emphasize the importance of completing the 5G-AKA for secure communication. By rejecting the request, the UE maintained the integrity and security of the communication process, preventing potential vulnerabilities that could arise from accepting a plain-text authentication request. Therefore, the UE's action was secure. Secure

23	23	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11994004249572754 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12018203735351562 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.32151198387145996 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is essential for establishing a secure communication context. Following this, 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, utilizing the 5G-EA0 (null) cipher algorithm and the 128-5G-IA2 integrity algorithm, with a security header indicating integrity protection with a new security context. However, the UE responded with a security mode reject message, citing an unspecified reason for rejection. The UE's decision to reject the security mode command could be considered secure based on the 5G standard outlined by 3GPP. The use of the 5G-EA0 (null) cipher algorithm means that no encryption was applied, which might have prompted the UE to reject the command to ensure the integrity and confidentiality of its communications. The UE's action aligns with the security principles of 5G, which prioritize the protection of user data and the establishment of a secure communication channel. Therefore, the UE's response to reject the security mode command due to the lack of encryption can be seen as a secure action, adhering to the 5G security standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was focused on the authentication process. Initially, the UE sent an authentication response to the AMF, which was followed by the AMF sending an authentication request back to the UE. Notably, the downlink message from the AMF was sent in plain text, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, as encryption of messages is contingent upon the successful completion of this procedure. The UE then responded with another authentication response. According to the 3GPP standards, the 5G-AKA procedure is crucial for establishing a secure communication channel, as it ensures mutual authentication and the derivation of security keys for encrypting subsequent messages. The fact that the AMF sent the authentication request in plain text suggests that the security context was not established, and the UE's response to this plain text message without encryption indicates a potential vulnerability. The UE should ideally not proceed with sensitive exchanges until a secure context is confirmed. Therefore, based on the 3GPP standards and the observed behavior, the action taken by the UE was insecure, as it engaged in communication without ensuring the completion of the 5G-AKA process and the establishment of a secure channel. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed during the NAS communication phase. The UE sent an authentication response to the AMF, which was followed by an authentication reject message from the AMF. Notably, the authentication reject message was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, meaning that encryption had not yet been established. Following the receipt of the authentication reject, the UE responded with a deregistration request, indicating that it was initiating a disconnection from the network. According to the 3GPP standards, the UE's action to deregister upon receiving an authentication reject is a standard and expected behavior, as it prevents further communication without proper authentication and encryption. This action helps to mitigate potential security risks by ensuring that the UE does not continue to communicate with the network in an unprotected state. Therefore, the UE's response to the authentication reject was appropriate and aligned with security protocols, as it ceased communication to avoid potential vulnerabilities. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "security mode complete" message, indicating that it had successfully established a secure communication mode with the AMF. Subsequently, the AMF sent a "deregistration request" to the UE, which was integrity protected and ciphered, ensuring that the message was both authenticated and encrypted. The UE responded with a "deregistration accept" message, acknowledging the request. The packet capture shows that the messages were exchanged with appropriate security headers, indicating that the communication was protected as per the 3GPP standards. The UE's actions, including the acceptance of the deregistration request, were consistent with the expected behavior in a secure communication scenario, as the messages were integrity protected and ciphered, ensuring confidentiality and integrity. Therefore, based on the 3GPP standards and the secure handling of messages, the UE's actions can be considered 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "security mode complete" message to the AMF, indicating that it had successfully established a secure communication channel. Subsequently, the AMF sent a "deregistration request" to the UE, which was integrity protected and ciphered, ensuring that the message was both authenticated and encrypted. The UE responded with a "deregistration accept" message, indicating compliance with the deregistration request. The packet capture shows that the messages were exchanged with appropriate security headers, suggesting that the communication was conducted securely. The UE's actions adhered to the 3GPP standards by ensuring that the messages were protected after the 5G-AKA process, which is crucial for maintaining the confidentiality and integrity of the communication. Therefore, based on the interaction and adherence to the 5G security standards, the UE's actions can be considered secure. Secure

28	28	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3232 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.16000795364379883 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602778434753418 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36232805252075195 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is a prerequisite for secure communication. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with the security mode. However, the AMF then sent a "security mode command" back to the UE, which was protected, indicating that the message was encrypted and integrity protected. The UE responded with a "security mode reject" message, specifying that the security mode was rejected for unspecified reasons. The packet capture shows that the UE acknowledged the downlink message but ultimately rejected the security mode. The use of the 128-5G-EA2 cipher algorithm and the 5G-IA0 (null) integrity algorithm suggests that while encryption was applied, integrity protection was not enforced, as 5G-IA0 is a null algorithm. According to the 3GPP standards, integrity protection is crucial for ensuring the authenticity and integrity of messages. The UE's decision to reject the security mode could be seen as a precautionary measure due to the lack of integrity protection, which aligns with the security principles of the 5G standard. Therefore, the UE's action to reject the security mode in the absence of proper integrity protection can be considered a secure response to maintain the integrity and authenticity of its communication. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After completing the 5G Authentication and Key Agreement (5G-AKA), the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with secure communication. However, the AMF then sent a "security mode command" back to the UE, which was protected but used null cipher and integrity algorithms (5G-EA0 and 5G-IA0), meaning no encryption or integrity protection was applied. The security header indicated that the message was integrity protected with a new security context. In response, the UE sent a "security mode reject" message, specifying that the security mode was rejected for unspecified reasons. According to the 3GPP 5G standards, the UE's action to reject the security mode command is appropriate and secure. The use of null algorithms for encryption and integrity protection is not secure, as it leaves the communication vulnerable to interception and tampering. By rejecting the security mode command, the UE adhered to the security principles of the 5G standard, which require robust encryption and integrity protection to ensure secure communication. Therefore, the UE's decision to reject the insecure security mode command was in line with maintaining the security integrity of the communication. Secure.

30	30	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected (1) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.16007494926452637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037607192993164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.364534854888916 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was focused on the NAS (Non-Access Stratum) security procedures. Initially, the 5G Authentication and Key Agreement (5G-AKA) was completed, which is a prerequisite for secure communication. The UE then sent a "security mode complete" message to the AMF, indicating that it accepted the security parameters, including the ciphering and integrity protection algorithms. Subsequently, the AMF sent a "security mode command" back to the UE, which was protected, as indicated by the security header being integrity protected. The UE responded again with a "security mode complete" message. The use of the 5G-EA7 ciphering algorithm and the 128-5G-IA2 integrity algorithm suggests that the communication was intended to be secure, adhering to the 3GPP standards for encryption and integrity protection. However, the sequence of messages raises a concern: typically, the "security mode command" should precede the "security mode complete" message from the UE, not follow it. This unusual sequence could imply a potential issue in the security procedure, as the UE should not send a "security mode complete" before receiving a "security mode command." This deviation from the expected protocol flow could expose the communication to vulnerabilities, as it suggests that the UE might have accepted security parameters without proper initiation from the AMF. Therefore, based on the 3GPP standards and the observed message sequence, the action taken by the UE appears to be insecure. Insecure

31	31	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3300 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.1600170135498047 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16026687622070312 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36418795585632324 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) involves a sequence of NAS (Non-Access Stratum) messages. Initially, the 5G Authentication and Key Agreement (5G-AKA) procedure is completed, which is a prerequisite for establishing a secure communication channel. The UE then sends a "security mode complete" message to the AMF, indicating that it has accepted the security parameters proposed by the AMF. Subsequently, the AMF sends a "security mode command" back to the UE, which is protected, suggesting that the message is encrypted and integrity-protected. The security header indicates that the message is integrity protected with a new security context, which is a positive sign of secure communication. However, the use of the 5G-IA0 (null) integrity algorithm is concerning because it implies that no integrity protection is applied, potentially exposing the communication to tampering. Finally, the UE sends a "deregistration request," which is a standard procedure but could be indicative of an issue if it was unexpected. Given the use of a null integrity algorithm, the communication lacks a critical layer of security, making it vulnerable to attacks. Therefore, despite the encryption, the absence of integrity protection renders the UE's actions insecure according to the 5G standard outlined by 3GPP. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After the completion of the 5G Authentication and Key Agreement (5G-AKA), the UE sent a "security mode complete" message to the AMF, indicating that it had successfully processed the security mode command and was ready to proceed with secure communication. However, the AMF then sent another "security mode command" to the UE, which was protected, indicating that it was both integrity protected and ciphered. The UE, however, did not respond to this subsequent security mode command. According to the 3GPP standards, once the 5G-AKA is completed, the UE and the network should establish a secure communication channel using agreed-upon ciphering and integrity protection algorithms. In this scenario, the UE's lack of response to the subsequent security mode command from the AMF could indicate a potential issue. The UE should have responded to maintain the security context, especially since the message was protected. The absence of a response from the UE suggests a failure to adhere to the expected secure communication protocol, which could expose the communication to potential security risks. Therefore, based on the 3GPP standards, the action taken by the UE in this test scenario appears to be insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a "security mode complete" message, indicating that the security procedures, specifically the 5G Authentication and Key Agreement (5G-AKA), were successfully completed. This step is crucial as it ensures that subsequent messages are encrypted and protected. Following this, the AMF sent a "gmm status" message to the UE, which was protected and included a 5GMM cause value of 6, indicating an "Illegal ME" (Mobile Equipment). In response, the UE sent a "Deregistration request" message, originating from the UE itself. The UE's action to deregister upon receiving a status message indicating an illegal ME suggests that it is adhering to security protocols by attempting to disconnect from the network when it detects a potential issue with its equipment status. This behavior aligns with the 3GPP standards, which emphasize the importance of maintaining secure and authenticated communication. The UE's decision to deregister can be seen as a precautionary measure to prevent any unauthorized access or potential security breaches. Therefore, based on the interaction and the UE's response to the AMF's message, the UE's actions can be considered secure according to the 5G standard outlined by 3GPP. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for secure communication. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it had successfully established a secure communication mode. The AMF then sent a "deregistration request" to the UE, which was integrity protected and ciphered, ensuring that the message was both encrypted and authenticated. The UE responded with a "deregistration accept" message, acknowledging the request. The packet capture shows that the messages were exchanged with appropriate security headers, indicating that the communication was protected as per the 3GPP standards. The UE's actions, including the acknowledgment of the deregistration request, were consistent with the expected behavior in a secure communication scenario. Given that the 5G-AKA was completed and the messages were protected, the UE's actions can be considered secure according to the 3GPP standards. 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 the test scenario, the interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) involved the UE sending a "security mode complete" message, followed by the AMF sending a "service accept" message. The 5G Authentication and Key Agreement (5G-AKA) process was completed prior to these exchanges, which is crucial for establishing a secure communication channel. The packet capture indicates that the uplink message from the UE included a "security mode complete" and a "registration request," while the downlink message from the AMF was a "service accept" and was sent as "Protected." This suggests that the messages were encrypted, as required by the 5G standard once the 5G-AKA process is completed. However, the UE did not provide a response to the "service accept" message, which could be a point of concern if it indicates a failure to acknowledge or process the message correctly. According to the 3GPP standards, the completion of the 5G-AKA process and the subsequent encryption of messages are essential for secure communication. Since the messages were protected and the 5G-AKA was completed, the UE's actions appear to align with the security requirements. However, the lack of response from the UE to the "service accept" message could be interpreted as a potential issue, but without further context, it is difficult to definitively assess its impact on security. Overall, based on the information provided, the UE's actions seem to be secure as per the 5G standard. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated the communication by sending a "registration complete" message to the AMF, indicating that it had successfully registered with the network. Subsequently, the AMF sent a "deregistration request" to the UE, which was integrity protected and ciphered, ensuring that the message was both authenticated and encrypted. The UE responded with a "deregistration accept" message, acknowledging the request from the AMF. The use of integrity protection and encryption in the downlink message from the AMF suggests adherence to the security protocols outlined by the 3GPP standards, which require that NAS messages be protected to prevent unauthorized access and tampering. The UE's response to the deregistration request was appropriate and aligned with the expected behavior in a secure communication environment. Given that the 5G-AKA process was completed, ensuring that subsequent messages were encrypted, and the UE's actions were consistent with the security requirements, the communication can be considered secure. Therefore, based on the interaction and adherence to the 3GPP standards, the action taken by the UE was secure. Secure
37	37	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5078079700469971 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5080060958862305 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Service accept 0.7117960453033447 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) followed a sequence of NAS (Non-Access Stratum) communications. Initially, the UE sent an "UplinkNASTransport" message with a "Registration complete" indication, which signifies that the UE has completed its registration process with the network. Following this, the AMF responded with a "Service accept" message, which was sent as a protected downlink message, indicating that the communication was encrypted, as required by the 5G-AKA (Authentication and Key Agreement) procedure. This encryption ensures that the messages are secure and not susceptible to interception or tampering. Subsequently, the UE sent a "Deregistration request (UE originating)" message, indicating its intention to disconnect from the network. The sequence of events suggests that the UE adhered to the 5G security standards outlined by 3GPP, as the communication was encrypted after the successful completion of the 5G-AKA procedure. The UE's actions, including the deregistration request, were conducted securely within the framework of the 5G security protocols. Therefore, based on the interaction and adherence to the 5G security standards, the UE's actions can be considered secure. Secure

38	38	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.5716309547424316 UE to AMF UplinkNASTransport, Registration complete 0.5718338489532471 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS message indicating "registration complete" to the AMF. In response, the AMF sent a downlink NAS message, specifically a "security mode command," which was protected and indicated the use of the ABBA value 3000, the cipher algorithm 5G-EA0 (null), and the integrity algorithm 128-5G-IA2. The security header was marked as "Integrity protected with new security context (3)," suggesting that the message was intended to be secure. However, the UE did not provide any response to this security mode command. According to the 3GPP standards, after the 5G-AKA process, the UE should respond to the security mode command to establish encryption and integrity protection for subsequent messages. The lack of response from the UE indicates a failure to complete the security procedure, leaving the communication potentially vulnerable. This lack of response could mean that the UE did not accept the security parameters or encountered an issue processing the command, which is not compliant with the expected secure behavior as per the 3GPP standards. Therefore, based on the interaction and the UE's lack of response, the action taken by the UE was insecure. Insecure
39	39	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.2683730125427246 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2686209678649902 AMF to UE SACK (Ack=12, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.476357936859131 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed to assess the security of the UE's actions. The process began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for ensuring that subsequent messages are encrypted and integrity protected. Following this, the UE sent an uplink NAS message indicating "registration complete" to the AMF. In response, the AMF sent a downlink NAS message, specifically a "configuration update command," which was protected with a security header indicating that it was both integrity protected and ciphered. The UE then responded with an uplink NAS message, "configuration update complete," confirming the receipt and processing of the configuration update command. The use of integrity protection and ciphering in the downlink message from the AMF suggests adherence to the 3GPP standards for secure communication, as these measures ensure that the message is both authentic and confidential. Given that the 5G-AKA was completed successfully, and the subsequent messages were protected as per the 3GPP standards, the actions taken by the UE appear to be secure. Therefore, based on the interaction and the security measures in place, the UE's communication can be considered "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed to assess the security of the UE's actions. The process began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for ensuring that subsequent messages are encrypted and integrity protected. Following this, the UE sent an uplink NAS message indicating "registration complete" to the AMF. In response, the AMF sent a downlink NAS message, specifically a "configuration update command," which was protected with a security header indicating that it was both integrity protected and ciphered. The UE then responded with an uplink NAS message, "configuration update complete," confirming the receipt and processing of the configuration update command. The use of integrity protection and ciphering in the downlink message from the AMF suggests adherence to the 3GPP standards for secure communication, as these measures are designed to protect against eavesdropping and tampering. Given that the 5G-AKA was completed successfully and the subsequent messages were protected, the actions taken by the UE appear to be secure according to the 3GPP standards. Therefore, based on the observed interaction and the security measures in place, the UE's communication can be considered "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a "registration complete" message, indicating the completion of the initial registration process. Subsequently, the AMF sent a "security mode command" to the UE, which was protected, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had been completed successfully. The security mode command was sent with a security header indicating integrity protection with a new security context, using the cipher algorithm 128-5G-EA2 and the integrity algorithm 128-5G-IA2. However, the UE did not respond to this security mode command, which is a critical step in establishing a secure communication channel. Instead, the UE sent an "InitialUEMessage" with a "Service request," which was subsequently rejected by the AMF with a "Service reject" message, citing that the UE identity could not be derived by the network. The lack of response to the security mode command suggests that the UE did not complete the needed security procedures to establish a secure communication channel as per the 3GPP 5G standards. This failure to respond appropriately to the security mode command indicates a potential security vulnerability, as the UE did not adhere to the expected protocol for securing communications. Therefore, based on the interaction and the 5G standard, the action taken by the UE was insecure. Insecure
42	42	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.513239860534668 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5140058994293213 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5144908428192139 AMF to UE DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. The test began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for ensuring that subsequent NAS (Non-Access Stratum) messages are encrypted. Following this, the UE sent an uplink NAS transport message to the AMF. In response, the AMF sent a deregistration accept message back to the UE, which was protected, indicating that it was encrypted as per the 5G security standards. However, the UE did not provide any response to this deregistration accept message. The packet capture shows that the UE sent multiple uplink messages, including a PDU session establishment request, and the AMF responded with a configuration update command before sending the deregistration accept message. The lack of response from the UE to the deregistration accept message could be a point of concern, as it might indicate that the UE did not handle the message as expected. According to the 3GPP standards, the UE should acknowledge such messages to ensure proper session management and security compliance. The absence of a response from the UE suggests a potential security issue, as it may not be adhering to the expected protocol behavior, which could lead to vulnerabilities. Therefore, based on the observed interaction and the lack of response from the UE, the action taken by the UE appears to be insecure. Insecure

43	43	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5069518089294434 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5071558952331543 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5073068141937256 AMF to UE DownlinkNASTransport 0.7109389305114746 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed to assess the security of the UE's actions. Initially, the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is a prerequisite for secure communication, ensuring that subsequent messages are encrypted and integrity protected. The UE sent an uplink NAS transport message, followed by the AMF sending a configuration update command, which was protected with integrity protection and ciphering, as indicated by the security header. This protection is crucial as it ensures that the message is both confidential and authentic, preventing unauthorized access or tampering. The UE then sent a deregistration request, which is a standard procedure when the UE wishes to disconnect from the network. Given that the 5G-AKA was completed and the messages were protected, the UE's actions align with the 3GPP standards for secure communication. The use of encryption and integrity protection indicates that the UE maintained a secure communication channel with the AMF, adhering to the security protocols established for 5G networks. Therefore, based on the observed interaction and adherence to the 5G security standards, the UE's actions can be considered secure. Secure
44	44	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 6.589772939682007 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 6.5903379917144775 AMF to UE SACK (Ack=18, Arwnd=106401) , DownlinkNASTransport, Configuration update command 6.590748071670532 AMF to UE DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 6.793751955032349 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated an uplink NAS transport message, which was followed by the AMF sending a deregistration request to the UE. This deregistration request was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered. The UE responded with a deregistration accept message, indicating that it acknowledged the deregistration request. The fact that the deregistration request from the AMF was protected suggests that the communication was encrypted and integrity-protected, as required by the 5G standard outlined by 3GPP. This protection ensures that the message was not tampered with and that it was confidential. The UE's response to the deregistration request was appropriate and aligned with the expected behavior in a secure communication scenario. Given that the 5G-AKA process was completed, and the subsequent messages were protected, the actions taken by the UE can be considered secure according to the 5G standard. Therefore, the communication between the UE and the AMF was secure. Secure

45	45	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5155510902404785 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5157649517059326 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5159080028533936 AMF to UE DownlinkNASTransport, Configuration update command 0.7195420265197754 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed to assess the security of the UE's actions. The test began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for secure communication, ensuring that subsequent messages are encrypted and integrity protected. Following this, the UE sent an uplink NAS transport message to the AMF. In response, the AMF sent a configuration update command back to the UE, which was protected with integrity protection and ciphering, as indicated by the security header. The UE then acknowledged this with a configuration update complete message. The packet capture confirms that the messages were exchanged in the expected sequence, with the downlink message from the AMF being protected, which aligns with the 3GPP standards for secure communication. Given that the 5G-AKA was completed and the messages were integrity protected and ciphered, the UE's actions adhered to the security protocols outlined by the 3GPP. Therefore, the communication between the UE and the AMF can be considered secure. Secure
46	46	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 2.425251007080078 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4254679679870605 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4255969524383545 AMF to UE DownlinkNASTransport, Configuration update command 2.629240036010742 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed to ensure compliance with the 5G security standards outlined by 3GPP. The test began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for secure communication, ensuring that both the UE and the network have established mutual authentication and derived the necessary security keys. Following this, the UE sent an uplink NAS transport message, which was acknowledged by the AMF with a configuration update command. The critical aspect of this interaction is that the downlink message from the AMF was sent as "Protected," with a security header indicating that it was both integrity protected and ciphered. This means that the message was encrypted and its integrity was verified, preventing unauthorized access or tampering. The UE responded with a configuration update complete message, indicating successful receipt and processing of the command. Given that the communication was conducted under the protection of the 5G-AKA security framework, and the messages were both encrypted and integrity protected, the actions taken by the UE adhered to the security standards set by 3GPP. Therefore, the communication between the UE and the AMF can be considered 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed to assess the security of the UE's communication. The process began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for ensuring that subsequent messages are encrypted and integrity protected. Following this, the UE sent an uplink NAS transport message to the AMF. In response, the AMF sent a configuration update command back to the UE, which was noted to be protected with a security header indicating that the message was both integrity protected and ciphered. The UE then acknowledged this with a configuration update complete message. The packet capture from Wireshark confirms these exchanges, showing that the messages were appropriately sequenced and protected after the 5G-AKA was completed. According to the 3GPP standards, the use of integrity protection and ciphering is essential for securing NAS messages, and the UE's actions adhered to these requirements. Therefore, based on the observed interaction and adherence to the 5G security standards, the UE's communication can be considered 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) was completed, which is a prerequisite for secure communication. Following this, the UE sent an uplink NAS transport message, and the AMF responded with a security mode command, which was protected and included a new security context. The security mode command from the AMF was intended to establish security parameters, including the ciphering and integrity algorithms (5G-EA4 and 128-5G-IA2, respectively). However, the UE responded with a security mode reject message, citing an unspecified reason. This rejection indicates that the UE did not accept the security parameters proposed by the AMF. According to the 3GPP standards, the UE should reject a security mode command if it detects any issues or inconsistencies with the proposed security context, such as unsupported algorithms or potential security threats. The UE's action to reject the security mode command, despite the lack of a specified reason, suggests that it adhered to the security protocols by not accepting potentially insecure or unsupported configurations. Therefore, based on the 3GPP standards, the UE's action can be considered secure, as it prioritized maintaining a secure communication channel by rejecting a potentially problematic security mode command. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF responded with a security mode command, which was sent as a protected downlink message. The security mode command included the use of the 5G-EA0 ciphering algorithm, which is a null cipher, and the 128-5G-IA2 integrity algorithm. The security header indicated that the message was integrity protected with a new security context. However, the UE responded with a security mode reject message, citing an unspecified reason for rejection. According to the 3GPP standards, the UE is expected to accept the security mode command if it is valid and properly protected. The use of the null cipher (5G-EA0) is typically not recommended for secure communications, as it implies no encryption, which could be a reason for the UE's rejection. The UE's decision to reject the security mode command could be seen as a protective measure against a potentially insecure configuration, especially if the null cipher was not expected or desired in the security context. Therefore, the UE's action to reject the security mode command, given the use of a null cipher, aligns with maintaining security standards by not accepting potentially insecure configurations. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request message to the AMF. This uplink message was part of the Non-Access Stratum (NAS) communication, which should be protected if the 5G Authentication and Key Agreement (5G-AKA) procedure has been completed successfully. The AMF, under test control, responded with a deregistration accept message, which was sent as a protected downlink message. Notably, the UE did not provide any response to this deregistration accept message. According to the 3GPP standards, once the 5G-AKA procedure is completed, all subsequent NAS messages should be encrypted and integrity protected to ensure secure communication. The fact that the UE did not respond to the deregistration accept message could indicate a lack of proper handling of the message, which might be due to the message being unexpected or improperly processed. However, since the message from the AMF was protected, it suggests that the communication channel was secure. The absence of a response from the UE does not necessarily imply insecurity, but it does raise questions about the UE's handling of unexpected or unsolicited messages. Overall, the interaction appears to be secure in terms of message protection, but the UE's lack of response could be a point of concern for robustness rather than security. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. This indicates that the initial security procedures were successfully completed, allowing for secure communication. Following the service request, the AMF sent a deregistration request to the UE, which was protected with integrity protection and ciphering, as indicated by the security header. The UE responded with a deregistration accept message, acknowledging the deregistration request. The key point of analysis here is the UE's response to the deregistration request. According to the 3GPP standards, the UE should only accept deregistration requests that are valid and expected within the protocol state. The test notes that the message type was not compatible with the protocol state, suggesting that the deregistration request was unexpected or inappropriate in this context. Despite this, the UE proceeded to accept the deregistration, which could be considered a security vulnerability, as it indicates that the UE did not adequately verify the legitimacy of the deregistration request. This behavior could potentially be exploited in a real-world scenario to disrupt service. Therefore, based on the 3GPP standards and the observed behavior, the action taken by the UE was insecure. Insecure
52	52	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 11.176167011260986 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 11.17656421661377 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command 11.383517980575562 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for secure communication. Following this, the UE sent a service request to the AMF, which is a standard procedure for initiating communication or requesting services. The AMF responded with a configuration update command, which was sent as a protected message, indicating that it was both integrity protected and ciphered, as per the security header information. This ensures that the message was encrypted and protected against tampering, aligning with the 3GPP standards for secure communication. Subsequently, the UE sent a deregistration request, which was also transmitted securely as part of the uplink NAS transport. The sequence of actions taken by the UE, including the initial service request and the subsequent deregistration request, were conducted under the protection of the 5G-AKA security framework, ensuring that all communications were encrypted and integrity protected. This adherence to the 3GPP security standards suggests that the UE's actions were secure. Therefore, based on the outlined interaction and the security measures in place, the UE's communication can be considered "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request to the AMF. Following this, the AMF responded with a deregistration request, which was sent as a protected message with integrity protection and ciphering, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had been completed successfully. The UE then responded with a deregistration accept message, acknowledging the deregistration request. The sequence of events shows that the UE adhered to the expected protocol by first completing the 5G-AKA, ensuring that subsequent messages were encrypted and integrity-protected. The UE's response to the deregistration request was appropriate, as it provided a deregistration accept message, which is a standard procedure when receiving such a request. The use of encryption and integrity protection aligns with the 3GPP standards for secure communication in 5G networks. Therefore, based on the actions taken by the UE and the adherence to the security protocols outlined by 3GPP, the UE's communication can be considered secure. Secure
54	54	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 100 UE provided: No response The packet capture during the test using wireshark is: 1.321023941040039 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 1.3216829299926758 AMF to UE DownlinkNASTransport, 5GMM status (Conditional IE error) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF responded with a GMM status message, which was sent as a protected downlink message. The 5GMM Cause code provided was 100, indicating a conditional IE error. Notably, the UE did not provide any response to the GMM status message from the AMF. According to the 3GPP standards, once the 5G-AKA process is completed, all subsequent NAS messages should be encrypted to ensure secure communication. The fact that the AMF's message was protected aligns with this requirement. However, the UE's lack of response to the GMM status message could be a point of concern. In a secure communication scenario, the UE is expected to handle and respond to such messages appropriately, especially when they are protected. The absence of a response from the UE might indicate a failure to process the message correctly, which could be considered a deviation from secure communication practices as outlined by the 3GPP standards. Therefore, based on the UE's actions, the communication can be considered "Insecure."

55	55	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003898143768310547 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an initial registration request to the AMF. In response, the AMF sent an authentication reject message back to the UE. Notably, this downlink message was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed. The UE did not provide any response to the authentication reject message. According to the 3GPP standards, the 5G-AKA procedure is crucial for establishing a secure communication channel, as it ensures that messages are encrypted and authenticated. Since the 5G-AKA was not completed, the communication remained unencrypted, leaving it vulnerable to interception and tampering. The UE's lack of response to the authentication reject could be seen as a passive approach, but it does not mitigate the risk posed by the unencrypted message. Therefore, based on the 3GPP standards, the UE's action in this scenario is considered insecure due to the absence of encryption and authentication in the communication. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an initial registration request to the AMF. Subsequently, the AMF responded with an authentication reject message, which was sent in plain text. The UE did not provide any response to this message. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to establish a secure communication channel, ensuring that messages are encrypted. In this scenario, the 5G-AKA was not completed, and the AMF's authentication reject message was sent unencrypted. The UE's lack of response to the plain-text authentication reject message is consistent with secure behavior, as it avoids engaging further in an insecure communication channel. By not responding, the UE mitigates the risk of potential security vulnerabilities that could arise from processing or responding to unencrypted messages. Therefore, based on the 3GPP standards and the actions taken by the UE, the UE's behavior can be considered secure in this context. Secure

57	57	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003440380096435547 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. This uplink message was part of the Non-Access Stratum (NAS) communication, which is crucial for establishing a connection in a 5G network. However, the AMF responded with an authentication reject message, which was sent in plain text. The 5G Authentication and Key Agreement (5G-AKA) procedure, which is essential for securing NAS messages, had not been completed at this point. As a result, the UE did not provide any response to the authentication reject message. According to the 3GPP standards, the 5G-AKA procedure must be completed to ensure that subsequent messages are encrypted and secure. Since the authentication reject message was sent in plain text and the UE did not respond, it indicates that the UE did not proceed with any further actions that could compromise security. The lack of response from the UE suggests that it adhered to the security protocols by not engaging further without a secure channel being established. Therefore, based on the 3GPP standards, the UE's action of not responding to an unencrypted message before the completion of 5G-AKA can be 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an initial registration request to the AMF. Following this, the AMF responded with an authentication reject message, which was sent in plain text. The UE did not provide any response to this message. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to establish a secure communication channel, ensuring that subsequent messages are encrypted. In this scenario, the 5G-AKA was not completed, and the AMF's authentication reject message was sent unencrypted. The UE's lack of response to the plain-text authentication reject message is consistent with secure behavior, as it avoids engaging further in an insecure communication channel. By not responding, the UE mitigates the risk of potential security vulnerabilities that could arise from processing or responding to unencrypted messages. Therefore, based on the 3GPP standards and the actions taken by the UE, the UE's behavior can be considered secure in this context. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was initiated with the UE sending an initial registration request. This uplink message was followed by a downlink message from the AMF, which was an authentication reject sent in plain text. The UE did not provide any response to this message. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to establish a secure communication channel, ensuring that subsequent messages are encrypted. In this scenario, the 5G-AKA was not completed, and the AMF's message was sent in plain text, which is a typical behavior before security contexts are established. The UE's lack of response to the authentication reject is consistent with the expected behavior, as it should not proceed with any further communication without successful authentication. This behavior aligns with the security protocols outlined by 3GPP, as the UE did not engage in any further communication that could compromise security. Therefore, the UE's action in this scenario can be considered secure. Secure
60	60	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0003459453582763672 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request to the AMF. Following this, the AMF responded with an authentication reject message, which was sent in plain text. The UE did not provide any response to this message. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to establish a secure communication channel, ensuring that subsequent messages are encrypted. In this scenario, the 5G-AKA was not completed, and the AMF's authentication reject message was sent unencrypted. The UE's lack of response to the plain-text authentication reject message is consistent with secure behavior, as it avoids engaging further in an insecure communication channel. By not responding, the UE mitigates the risk of potential security vulnerabilities that could arise from processing or responding to unencrypted messages. Therefore, based on the 3GPP standards and the actions taken by the UE, the UE's behavior can be considered secure in this context. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an initial registration request to the AMF. In response, the AMF sent a registration reject message back to the UE. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure was not completed, which is crucial for establishing a secure communication channel. The registration reject message from the AMF was sent in plain text, indicating that encryption was not applied, as encryption relies on the successful completion of the 5G-AKA process. The 5GMM Cause code 111, which corresponds to a "Protocol error, unspecified," suggests that the rejection was due to a protocol-related issue. The UE did not provide any response to the registration reject message. According to the 3GPP standards, the lack of encryption in the communication between the UE and the AMF, due to the incomplete 5G-AKA process, exposes the interaction to potential security vulnerabilities. Therefore, the action taken by the UE, in this case, is considered insecure because it did not ensure the confidentiality and integrity of the communication as required by the 5G security standards. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF responded with a deregistration accept message, which was sent as a protected downlink message. The UE, however, did not provide any response to this message. According to the 3GPP standards, once the 5G-AKA process is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF's deregistration accept message was protected indicates that the message was encrypted, adhering to the security requirements. However, the UE's lack of response to the deregistration accept message raises concerns. In a typical scenario, the UE should acknowledge such a message to confirm receipt and understanding, ensuring a secure and synchronized communication process. The absence of a response from the UE could imply a potential issue in handling the message, which might expose vulnerabilities in the UE's security implementation. Therefore, while the AMF's action was secure, the UE's lack of response suggests a potential insecurity in its communication process. Insecure.

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an authentication response, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure was completed. Following this, the AMF sent a security mode command to the UE, which was protected, as indicated by the security header stating "Integrity protected with new security context (3)." This implies that the message was both encrypted and integrity-protected, utilizing the specified cipher and integrity algorithms (128-5G-EA1 and 128-5G-IA2, respectively). The UE then sent a deregistration request, which was UE-originating, suggesting that the UE initiated the deregistration process. The sequence of events shows that the UE adhered to the 5G security procedures by first completing the 5G-AKA, ensuring that subsequent messages were protected. The use of encryption and integrity protection aligns with the 3GPP standards for secure communication. The UE's actions, including the deregistration request, appear to be in compliance with the security protocols, as it only proceeded with deregistration after establishing a secure context. Therefore, based on the outlined interaction and adherence to the 5G security standards, the UE's actions 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 the described security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with a service accept message. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to this exchange, which is a prerequisite for ensuring that subsequent NAS (Non-Access Stratum) messages are encrypted and integrity protected. The packet capture indicates that the service request from the UE was sent as an InitialUEMessage with a cause of mo-Data, and the AMF's response was a DownlinkNASTransport message containing a service accept, which was marked as "Protected." However, the UE did not provide any response to the AMF's service accept message. According to the 3GPP standards, after the 5G-AKA procedure, the UE should be able to process and respond to protected messages from the AMF. The lack of response from the UE suggests a potential issue in processing the protected message, which could indicate a failure in maintaining the expected security protocols. This lack of response could be due to several reasons, such as an inability to decrypt the message or a failure in the integrity check, both of which would be considered non-compliant with the 3GPP security standards. Therefore, based on the UE's failure to respond to a protected message after the 5G-AKA procedure, the action taken by the UE appears to be 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is a prerequisite for secure communication. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters previously negotiated. However, the AMF then sent a "security mode command" back to the UE, which was protected using the cipher algorithm 128-5G-EA2 and the integrity algorithm 128-5G-IA1, with the security header indicating integrity protection with a new security context. Despite this, the UE responded with a "security mode reject" message, citing an unspecified reason for rejection. This sequence of events suggests that the UE detected an anomaly or inconsistency in the security mode command, prompting it to reject the command to maintain security. According to the 3GPP standards, the UE is expected to reject any security mode command that does not align with the established security context or if it detects any potential security threats. Therefore, the UE's action to reject the security mode command, despite the lack of a specified reason, aligns with the security protocols designed to protect against unauthorized or potentially harmful commands. This cautious approach by the UE indicates adherence to the 5G security standards, ensuring that only legitimate and secure communications are accepted. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is essential for establishing a secure communication channel. Following this, the UE sent an uplink NAS transport message, and the AMF responded with a security mode command, which was protected and included a new security context. The security mode command from the AMF was intended to establish the security algorithms for ciphering and integrity protection, specifically using the 128-5G-EA1 cipher algorithm and the 128-5G-IA2 integrity algorithm. However, the UE responded with a security mode reject message, indicating that it did not accept the security mode command, citing an unspecified reason. According to the 3GPP standards, the UE's rejection of the security mode command could be considered secure if the UE detected any inconsistencies or potential security threats in the proposed security context or algorithms. The UE's action to reject the security mode command, despite the completion of the 5G-AKA, suggests a cautious approach to ensuring the integrity and confidentiality of its communication. Therefore, based on the information provided and the 3GPP standards, the UE's action can be considered secure, as it prioritized maintaining a secure communication channel by rejecting a potentially insecure security mode. Secure

67	67	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 98 UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.8137481212615967 UE to AMF UplinkNASTransport, Service request 0.814223051071167 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Unknown) 1.0217480659484863 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After completing the 5G Authentication and Key Agreement (5G-AKA), the UE sent a service request to the AMF. In response, the AMF sent a GMM (GPRS Mobility Management) status message back to the UE, which was protected, indicating that encryption was applied as expected after the 5G-AKA completion. The GMM status message from the AMF included a 5GMM Cause value of 98, which typically indicates a protocol error or an unexpected message. The UE then responded with a 5GMM status message indicating that the message type was not compatible with the protocol state. This response from the UE suggests that it correctly identified an inconsistency or unexpected message type from the AMF, which aligns with the 3GPP standards for handling protocol errors. The UE's action to send a status message indicating the incompatibility demonstrates adherence to the protocol's error-handling procedures, ensuring that the communication remains secure by not proceeding with potentially erroneous or malicious instructions. Therefore, based on the 3GPP standards and the UE's response to the unexpected message, the action taken by the UE was secure. Secure
68	68	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.7269129753112793 UE to AMF UplinkNASTransport, Service request 0.7272160053253174 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.9349148273468018 UE to AMF UplinkNASTransport, Configuration update complete, UplinkNASTransport, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated the communication by sending a service request to the AMF, which then responded with a configuration update command. This downlink message from the AMF was integrity protected, as indicated by the security header, ensuring that the message was not tampered with during transmission. The UE subsequently acknowledged the configuration update by sending a "Configuration update complete" message back to the AMF. The packet capture shows that the messages were exchanged in a timely manner, with the initial service request and the subsequent configuration update complete message being sent by the UE. Since the 5G-AKA process was completed prior to these exchanges, it can be inferred that the security context was established, allowing for the protection of NAS messages. The integrity protection of the downlink message from the AMF further supports the security of the communication. Based on the 3GPP standards, the actions taken by the UE appear to adhere to the security requirements, as the messages were protected following the successful completion of the 5G-AKA. Therefore, the communication between the UE and the AMF can be considered 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is crucial for establishing a secure communication channel. Following this, the UE sent an authentication response to the AMF, which then replied with a security mode command. This command was sent as a protected downlink message, indicating that it was integrity protected with a new security context, using the 128-5G-IA2 integrity algorithm and the 5G-EA0 ciphering algorithm (null ciphering). However, the UE responded with a security mode reject message, citing an unspecified reason for rejection. The UE's decision to reject the security mode command could be seen as a cautious approach, potentially due to a mismatch in security parameters or an inability to verify the integrity of the command. According to the 3GPP standards, the UE is expected to ensure that the security mode command is valid and that the security context is correctly established before proceeding. The rejection indicates that the UE did not accept the security parameters, which could be a protective measure against a potential security threat or misconfiguration. Therefore, the UE's action aligns with the 3GPP standards for maintaining secure communication, as it prioritized verifying the security context before accepting the command. Secure

70	70	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.547684907913208 UE to AMF UplinkNASTransport, Registration complete 0.5478739738464355 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "registration complete" message, followed by the AMF sending a "security mode command" to the UE. The security mode command was sent as a protected downlink message, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is a prerequisite for secure communication. The security mode command was protected with integrity and ciphered using a new security context, employing the 128-5G-IA2 integrity algorithm and the 5G-EA0 (null) ciphering algorithm. However, the UE did not respond to the security mode command. According to the 3GPP standards, after the 5G-AKA procedure, the UE should respond to the security mode command to establish a secure communication channel. The lack of response from the UE suggests a failure to comply with the expected security procedures, potentially leaving the communication vulnerable. Therefore, based on the 3GPP standards, the UE's action in this scenario can be considered insecure, as it did not complete the necessary steps to ensure a secure communication channel with the AMF. Insecure

71	71	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0332 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 4.62968111038208 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 4.630121946334839 AMF to UE SACK (Ack=10, Arwnd=106361) , DownlinkNASTransport, Configuration update command 4.6305460929870605 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. After the completion of the 5G Authentication and Key Agreement (5G-AKA), the UE sent an uplink NAS transport message to the AMF. Subsequently, the AMF responded with a security mode command, which was sent as a protected message. The security mode command was intended to establish security settings, including the ciphering and integrity protection algorithms. The AMF used the cipher algorithm 128-5G-EA3 and the integrity algorithm 5G-IA0 (null), with the security header indicating that the message was both integrity protected and ciphered. However, the UE did not provide any response to the security mode command. According to the 3GPP standards, the UE should respond to the security mode command to establish secure communication. The lack of response from the UE suggests a failure to complete the security setup, leaving the communication potentially vulnerable. Therefore, based on the 3GPP standards, the UE's action in this scenario was insecure, as it did not adhere to the expected protocol for establishing secure communication with the AMF. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS transport message, and the AMF responded with a security mode command, which was protected and included a new security context. The security mode command from the AMF was intended to establish the security algorithms for ciphering and integrity protection, specifically using the 5G-EA5 cipher algorithm and the 128-5G-IA2 integrity algorithm. However, the UE responded with a security mode reject message, citing an unspecified reason. This rejection indicates that the UE did not accept the security parameters proposed by the AMF, which could be due to a mismatch in security capabilities or a perceived threat. According to the 3GPP standards, the UE's action to reject the security mode command can be considered secure if it detected an inconsistency or potential security risk in the proposed security context. By rejecting the command, the UE prevents the establishment of a potentially insecure communication channel. Therefore, based on the information provided and the 3GPP standards, the UE's action to reject the security mode command appears to be a secure response to a situation where the security parameters may not have aligned with its expectations or capabilities. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) was completed, which is a prerequisite for secure communication. The UE then sent a "security mode complete" message to the AMF, indicating that it accepted the security parameters. However, the AMF subsequently sent a "security mode command" back to the UE, which was protected and used the 5G-EA0 (null) cipher algorithm and the 128-5G-IA2 integrity algorithm. The security header indicated that the message was integrity protected with a new security context. In response, the UE sent a "security mode reject" message, citing an unspecified reason for rejection. This sequence of events suggests that the UE detected an anomaly or inconsistency in the security mode command, possibly due to the use of the 5G-EA0 (null) cipher algorithm, which does not provide encryption. According to the 3GPP standards, the UE is expected to reject security configurations that do not meet the required security criteria, such as the absence of encryption. Therefore, the UE's decision to reject the security mode command aligns with the 3GPP standards for maintaining secure communication. The UE's action was a precautionary measure to ensure that the communication remained secure, as it did not accept a potentially insecure configuration. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is essential for establishing a secure communication channel. Following this, 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 it was integrity protected with a new security context, using the specified cipher and integrity algorithms (128-5G-EA3 and 128-5G-IA2, respectively). However, the UE responded with a security mode reject message, citing an unspecified reason for the rejection. The UE's decision to reject the security mode command could be seen as a cautious approach, potentially due to a mismatch in security parameters or an inability to verify the integrity of the command. According to the 3GPP standards, the UE is expected to reject security mode commands if there are discrepancies or if the security context is not properly established. This behavior ensures that the UE does not proceed with potentially insecure communication. Therefore, the UE's action to reject the security mode command, despite being unspecified, aligns with the security protocols outlined by 3GPP, as it prevents the establishment of a potentially insecure connection. Secure

75	75	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0392 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 0.4745960235595703 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4750940799713135 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.47630810737609863 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS transport message to the AMF. Subsequently, the AMF responded with a security mode command, which was sent as a protected message. The security mode command is a critical step in the 5G security framework, as it establishes the encryption and integrity protection algorithms to be used for subsequent NAS messages. In this test, the AMF specified the use of the 5G-EA5 ciphering algorithm and the 128-5G-IA1 integrity algorithm, with the security header indicating that the message was integrity protected with a new security context. However, the UE did not provide a response to the security mode command. According to the 3GPP standards, the UE is expected to respond to the security mode command to confirm the security algorithms and complete the security setup. The lack of response from the UE indicates a failure to comply with the expected security procedures, leaving the communication potentially vulnerable. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario was insecure. Insecure
76	76	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.16002702713012695 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.16026616096496582 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response, followed by the AMF sending an identity request. The identity request from the AMF was sent in plain text, and it specifically requested the Subscription Concealed Identifier (SUCI) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to ensure that subsequent NAS messages are encrypted. Since the 5G-AKA was not completed, the messages were not encrypted, which is why the identity request was sent in plain text. The UE's lack of response to the identity request can be considered a secure action because responding to a plain text request with sensitive information like the SUCI could expose the UE to potential security risks. By not responding, the UE avoided transmitting sensitive information over an unencrypted channel, adhering to the security principles outlined by 3GPP. Therefore, the UE's action in this scenario was secure. Secure

77	77	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0004799365997314453 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request 0.20071196556091309 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. Following this, the AMF, which was under test control, sent an identity request to the UE. Notably, this identity request was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The AMF requested the Subscription Concealed Identifier (SUCI) from the UE, and the UE responded with an identity response. According to the 3GPP standards, the 5G-AKA procedure is crucial for establishing a secure communication channel, as it ensures that subsequent messages are encrypted. Since the 5G-AKA was not completed, the communication, including the identity request and response, was not encrypted, leaving the UE's identity potentially exposed. This exposure is contrary to the security principles outlined by 3GPP, which emphasize the importance of protecting subscriber identity and ensuring secure communication. Therefore, the action taken by the UE, in this case, was insecure, as it responded to an identity request in plain text without the protection of encryption. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) was completed, which is a prerequisite for secure communication. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with the security context. However, the AMF then sent a "security mode command" back to the UE, which was protected and used the 5G-EA0 (null) cipher algorithm and the 128-5G-IA2 integrity algorithm. The security header indicated that the message was integrity protected with a new security context. Despite this, the UE responded with a "security mode reject" message, citing an unspecified reason for rejection. This sequence of events suggests that the UE detected an issue with the security mode command, possibly due to the use of the null cipher algorithm (5G-EA0), which does not provide encryption. According to the 3GPP standards, the use of a null cipher algorithm is generally considered insecure for protecting user data, as it does not encrypt the data, leaving it vulnerable to interception. The UE's decision to reject the security mode command indicates that it adhered to security protocols by not accepting a potentially insecure configuration. Therefore, the UE's action was in line with maintaining security standards, as it refused to proceed with a security mode that did not meet the necessary encryption requirements. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is essential for establishing a secure communication channel. Following this, the UE sent an authentication response to the AMF, which then replied with a security mode command. This command was sent as a protected message, utilizing the 5G-EA0 (null) cipher algorithm and the 128-5G-IA2 integrity algorithm, with a security header indicating integrity protection with a new security context. However, the UE responded with a security mode reject message, citing an unspecified reason for rejection. The UE's decision to reject the security mode command could be considered secure based on the 3GPP standards if the UE detected any inconsistencies or potential security threats in the security mode command, such as the use of a null cipher algorithm (5G-EA0), which does not provide encryption. The integrity protection alone may not suffice for secure communication, especially if encryption is expected. Therefore, the UE's rejection of the security mode command could be a precautionary measure to prevent potential vulnerabilities. Based on this analysis, the UE's action aligns with maintaining security standards by not accepting potentially insecure configurations. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request, which was followed by the AMF responding with a configuration update command. The AMF's downlink message was protected, with the security header indicating that it was integrity protected with a new security context. This suggests that the 5G Authentication and Key Agreement (5G-AKA) procedure was completed successfully, establishing a secure communication channel. However, the UE responded with a 5GMM status message indicating that the message type was not compatible with the protocol state. This response from the UE suggests that it detected an inconsistency or unexpected message type, which could be a security measure to prevent processing potentially malicious or erroneous messages. According to the 3GPP standards, the UE's action to reject or flag unexpected messages is a security feature designed to maintain protocol integrity and prevent unauthorized access or manipulation. Therefore, the UE's response aligns with the security protocols outlined by 3GPP, as it ensures that only expected and valid messages are processed, thereby maintaining the integrity and security of the communication. Secure

81	81	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 2222 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.1596660614013672 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1599440574645996 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. After the completion of the 5G Authentication and Key Agreement (5G-AKA) process, the UE sent an authentication response to the AMF. Subsequently, the AMF sent a security mode command back to the UE, which was protected with integrity protection, as indicated by the security header. The ciphering and integrity algorithms used were 5G-EA0 and 5G-IA0, respectively, both of which are null algorithms, meaning no encryption or integrity protection was applied. The UE, however, did not provide any response to the security mode command. According to the 3GPP standards, after the 5G-AKA process, the UE should respond to the security mode command to establish secure communication channels. The lack of response from the UE indicates a failure to proceed with the necessary security procedures, leaving the communication unprotected. This behavior is considered insecure as it does not comply with the 3GPP standards for secure communication in 5G networks, which require the establishment of encryption and integrity protection after authentication. Therefore, the UE's action in this scenario is deemed insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is crucial for establishing a secure communication channel. Following this, the UE sent an authentication response to the AMF, which then responded with a security mode command. This command was sent as a protected downlink message, indicating that the AMF intended to establish a secure communication context using the specified cipher and integrity algorithms. However, the UE responded with a security mode reject message, citing an unspecified reason for the rejection. The security mode command from the AMF used the cipher algorithm 128-5G-EA3 and the integrity algorithm 5G-IA0 (null), with a security header indicating integrity protection with a new security context. The UE's rejection of the security mode command suggests that it did not accept the proposed security parameters, possibly due to the use of the null integrity algorithm, which does not provide integrity protection. According to the 3GPP standards, integrity protection is a critical component of secure communication, and the absence of it could be a reason for the UE to reject the security mode. Therefore, the UE's action to reject the security mode command can be considered secure, as it adhered to the principle of ensuring robust security measures before proceeding with communication. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with a service accept message. The test indicates that the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is a prerequisite for ensuring that subsequent NAS (Non-Access Stratum) messages are encrypted and integrity protected. The packet capture shows that the service request was sent from the UE to the AMF, and the AMF responded with a service accept message that was marked as "Protected," indicating that it was encrypted. However, the UE did not provide any response to the service accept message. According to the 3GPP standards, after the 5G-AKA procedure, the UE should be able to process and respond to protected messages from the AMF. The lack of response from the UE could suggest a failure in processing the encrypted message, which may indicate a potential issue with the UE's handling of secure communications. This could be due to a misconfiguration, a software bug, or an issue with the encryption keys. Given that the UE did not respond to a protected message after the 5G-AKA was completed, it suggests a deviation from the expected secure behavior as per the 3GPP standards. Therefore, based on the observed interaction, the UE's action appears to be insecure. Insecure

84	84	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0083 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.11982488632202148 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12009406089782715 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3228750228881836 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is essential for establishing a secure communication channel. Following this, the UE sent an authentication response to the AMF, which then replied with a security mode command. This command was sent as a protected message, indicating that it was integrity protected with a new security context, using the specified cipher and integrity algorithms (128-5G-EA2 and 128-5G-IA2, respectively). However, the UE responded with a security mode reject message, citing an unspecified reason for the rejection. The UE's decision to reject the security mode command could be seen as a precautionary measure, potentially due to a mismatch in security parameters or an inability to verify the integrity of the message. According to the 3GPP standards, the UE is expected to reject security mode commands if there are any discrepancies or security concerns, to prevent potential vulnerabilities. Therefore, the UE's action to reject the command, despite the lack of a specified reason, aligns with the security protocols outlined by 3GPP, as it prioritizes maintaining a secure communication environment. Based on this analysis, the UE's actions can be considered secure. Secure

85	85	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.16005301475524902 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16028904914855957 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.36393094062805176 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is a prerequisite for secure communication. Following this, the UE sent a "security mode complete" message to the AMF, indicating its readiness to proceed with the security mode. However, the AMF then sent a "security mode command" back to the UE, which was protected, indicating that it was integrity protected with a new security context. The UE responded with a "security mode reject" message, citing an unspecified reason for rejection. The use of the 5G-EA0 (null) ciphering algorithm and 5G-IA0 (null) integrity algorithm suggests that no encryption or integrity protection was applied, which is typically used for testing or when no security is required. The UE's rejection of the security mode command could be interpreted as a precautionary measure, possibly due to the use of null algorithms or an unexpected security context. According to the 3GPP standards, the UE should reject any security mode command that does not meet the expected security requirements or if there is any inconsistency in the security context. Therefore, the UE's action to reject the security mode command, given the unspecified reason and the use of null algorithms, aligns with maintaining security integrity as per the standards. Thus, the UE's response can be considered secure. Secure

86	86	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected and ciphered (2) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.15096688270568848 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15124177932739258 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.35789990425109863 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. Initially, the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is a prerequisite for secure communication. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters and was ready to proceed with secure communication. However, the AMF then sent a "security mode command" back to the UE, which was protected, indicating that the message was both integrity protected and ciphered. The UE responded again with a "security mode complete" message. The use of the cipher algorithm 128-5G-EA1 and integrity algorithm 128-5G-IA2, along with the security header indicating integrity protection and ciphering, suggests that the communication was conducted under the security protocols outlined by the 3GPP standards. The UE's actions, including the repeated sending of "security mode complete" messages, suggest that it adhered to the expected security procedures by ensuring that the communication was protected after the 5G-AKA was completed. Given that the messages were encrypted and integrity protected, the UE's actions appear to be secure according to the 5G standard. Therefore, the UE's communication can be considered "Secure."

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF responded with a deregistration request, which was integrity protected and ciphered, indicating that the message was secured according to the 5G standards. However, the UE's subsequent response included a 5GMM status message indicating "Invalid mandatory information," which suggests that the UE did not handle the deregistration request appropriately. The UE then sent another service request, which was followed by a service reject message from the AMF, stating that the "UE identity cannot be derived by the network." This sequence of events indicates that the UE failed to process the deregistration request correctly, leading to an invalid response. According to the 3GPP standards, the UE should have properly handled the deregistration request, especially since the message was protected. The UE's failure to do so and the subsequent invalid information response suggest a potential security flaw in the UE's handling of protected messages. Therefore, based on the 3GPP standards, the UE's actions in this scenario were insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response, followed by the AMF sending an identity request. The identity request from the AMF was sent in plain text, and it specifically requested the Subscription Concealed Identifier (SUCI) from the UE. The UE responded with an identity response. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to establish a secure communication channel, which includes encryption of NAS messages. In this test, the 5G-AKA was not completed, meaning that the communication was not encrypted. The AMF's request for the SUCI in plain text and the UE's subsequent response without encryption exposes sensitive information, which is contrary to the security principles outlined by 3GPP. The SUCI is designed to protect the subscriber's permanent identifier (SUPI) and should be transmitted securely. Since the UE provided the identity response without the completion of 5G-AKA and encryption, the action taken by the UE was insecure according to the 3GPP standards. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed during the NAS communication phase. The UE sent an authentication response to the AMF, which is a standard step in the 5G-AKA (Authentication and Key Agreement) procedure. However, before the 5G-AKA process was completed, the AMF sent an identity request to the UE, requesting the Subscription Concealed Identifier (SUCI). Notably, this identity request was sent in plain text, as encryption of messages is contingent upon the completion of the 5G-AKA process. The UE responded with an identity response, providing the requested SUCI. According to the 3GPP standards, the SUCI is a privacy-preserving identifier that should be protected to prevent exposure of the subscriber's identity. Since the 5G-AKA process was not completed, the communication was not encrypted, leaving the SUCI potentially exposed to interception. This exposure of sensitive information before the establishment of a secure channel indicates a vulnerability in the UE's handling of identity requests. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario was insecure. Insecure
90	90	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: Identity response The packet capture during the test using wireshark is: 0.11975502967834473 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11999011039733887 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request 0.3266119956970215 UE to AMF UplinkNASTransport, Identity response This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the User Equipment (UE) engaged in a Non-Access Stratum (NAS) communication with the Access and Mobility Management Function (AMF) as part of a 5G standalone network security test. The UE sent an authentication response to the AMF, which is a standard step in the 5G Authentication and Key Agreement (5G-AKA) procedure. However, before the 5G-AKA process was completed, the AMF sent an identity request to the UE, requesting the Subscription Concealed Identifier (SUCI). Notably, this identity request was sent in plain text, as encryption of NAS messages is contingent upon the completion of the 5G-AKA process. The UE responded with an identity response, providing the requested SUCI. According to the 3GPP standards, the SUCI is a privacy-preserving identifier that should be protected to prevent exposure of the subscriber's identity. Since the 5G-AKA process was not completed, the communication was not encrypted, leaving the SUCI potentially exposed to interception. This exposure of sensitive information before the establishment of a secure channel indicates a deviation from the secure communication practices outlined by 3GPP. Therefore, the action taken by the UE in responding to an unencrypted identity request with sensitive information is considered insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request, which is a standard procedure following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF, under controlled test conditions, responded with a deregistration request, indicating an "Illegal UE" status. This message was sent as a protected downlink message, with integrity protection and ciphering applied, as indicated by the security header. The UE then responded with a 5GMM status message, indicating "Invalid mandatory information." This response suggests that the UE detected an anomaly or inconsistency in the deregistration request, which could be due to the test conditions where the AMF was simulating an illegal UE scenario. According to the 3GPP standards, the UE's response to an unexpected or invalid message should be to maintain the integrity and confidentiality of its communications, which it did by sending a status message indicating the invalidity of the received information. This behavior aligns with the security principles outlined in the 5G standards, as the UE did not proceed with any deregistration process that could compromise its security. Therefore, based on the interaction and the UE's adherence to the expected security protocols, the action taken by the UE can be considered secure. Secure
92	92	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.7997009754180908 UE to AMF UplinkNASTransport, Service request 0.7998991012573242 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 1.0037281513214111 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request to the AMF. Following this, the AMF responded with a deregistration request, which was integrity protected and ciphered, indicating that the message was secured according to the 5G security standards. The UE then sent a deregistration accept message back to the AMF, completing the communication sequence. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to these exchanges, ensuring that the messages were encrypted and integrity protected. According to the 3GPP standards, the UE's actions appear to be secure as it adhered to the protocol by responding appropriately to the deregistration request with a deregistration accept message. The use of integrity protection and ciphering for the downlink message from the AMF further supports the security of the communication. Therefore, based on the outlined interaction and adherence to the 5G security standards, the UE's actions can be considered 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) was completed, which is a prerequisite for secure communication. The UE then sent a "security mode complete" message to the AMF, indicating its readiness to proceed with the agreed security parameters. However, the AMF subsequently sent a "security mode command" message, which was protected, indicating that it was encrypted and integrity-protected using the new security context. The UE responded with a "security mode reject" message, citing a mismatch in UE security capabilities. This indicates that the UE detected a discrepancy between its security capabilities and the security requirements specified by the AMF. The UE's action to reject the security mode command is consistent with the 3GPP standards, which emphasize the importance of matching security capabilities to prevent potential vulnerabilities. By rejecting the command due to a mismatch, the UE is adhering to the security protocols designed to protect against unauthorized or insecure configurations. Therefore, the UE's action in this scenario was secure, as it prevented the establishment of a potentially insecure communication channel. 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 User Equipment (UE) initiated a registration process by sending an initial registration request to the Access and Mobility Management Function (AMF). In response, the AMF sent an identity request to the UE, requesting the Subscription Concealed Identifier (SUCI). The identity request from the AMF was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The UE then responded with an identity response. According to the 3GPP standards, the 5G-AKA procedure must be completed before any NAS messages can be encrypted, ensuring the confidentiality and integrity of the communication. Since the 5G-AKA was not completed, the communication between the UE and AMF, specifically the identity request and response, was not encrypted. This lack of encryption exposes the UE to potential security risks, as sensitive information like the SUCI could be intercepted by malicious entities. Therefore, based on the 3GPP standards, the action taken by the UE in responding to an unencrypted identity request without the completion of 5G-AKA is considered insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request, which is a standard procedure following the completion of the 5G Authentication and Key Agreement (5G-AKA). The AMF then responded with a deregistration request, which was integrity protected and ciphered, indicating that the message was encrypted and authenticated, as required by the 5G security standards. The UE subsequently sent a deregistration accept message, acknowledging the deregistration request. The key point of analysis here is the UE's response to the deregistration request. According to the 3GPP standards, the UE should only accept a deregistration request if it is valid and expected. In this test, the deregistration request was sent as a part of a controlled test scenario, and the message type was noted as not compatible with the protocol state, suggesting an anomaly. However, since the message was protected, the UE's acceptance of the deregistration request indicates that it adhered to the security protocols by ensuring the message was authenticated and encrypted before responding. Therefore, despite the unusual nature of the test scenario, the UE's actions were consistent with the security requirements of the 5G standard, as it only responded to a protected message. 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 the test scenario, the User Equipment (UE) engaged in a Non-Access Stratum (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. Subsequently, the AMF sent an identity request back to the UE, which was transmitted in plain text, requesting the Subscription Concealed Identifier (SUCI). The UE then provided another identity response. According to the 3GPP standards, for messages between the UE and the AMF to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed. In this test, the 5G-AKA was not completed, meaning that the communication was not encrypted. The UE's action of responding to an identity request sent in plain text without the completion of 5G-AKA exposes the communication to potential interception and eavesdropping, which is not secure according to the 5G security standards. The UE should ideally wait for the 5G-AKA to be completed to ensure that the communication is encrypted and secure. Therefore, based on the interaction and the lack of encryption, the action taken by the UE is considered insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the exchange of NAS messages. Initially, the UE sent an identity response to the AMF, which was followed by an identity request from the AMF. Notably, the identity request from the AMF was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed yet. The AMF requested the Subscription Concealed Identifier (SUCI) from the UE, and the UE responded with an identity response. According to the 3GPP standards, the 5G-AKA procedure must be completed to establish a secure communication channel, ensuring that subsequent messages are encrypted. Since the 5G-AKA was not completed, the communication between the UE and AMF was not encrypted, leaving the identity request and response vulnerable to interception. The UE's action of responding to an unencrypted identity request with sensitive information like the SUCI is considered insecure, as it exposes the UE to potential security risks. Therefore, based on the 3GPP standards, the UE's communication in this scenario was insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request, which is a standard procedure following the completion of the 5G Authentication and Key Agreement (5G-AKA). The AMF responded with a configuration update command, which was integrity protected with a new security context, indicating that the message was secured according to the 5G security standards. However, the UE responded with a 5GMM status message indicating that the message type was not compatible with the protocol state. This response suggests that the UE detected an inconsistency or unexpected message type, which could be a result of a protocol mismatch or an error in the message sequence. According to the 3GPP standards, the UE's action to send a 5GMM status message in response to an unexpected or incompatible message type is a security measure to prevent potential protocol misuse or attacks. By identifying and flagging the message as incompatible, the UE is adhering to the security protocols designed to maintain the integrity and confidentiality of the communication. Therefore, the UE's action in this scenario aligns with the 5G security standards and demonstrates a secure response to an unexpected situation. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an uplink NAS transport message, followed by the AMF responding with a service accept message. The test indicates that the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is a prerequisite for ensuring that subsequent NAS messages are encrypted and integrity protected. The packet capture shows that the uplink message from the UE was a PDU session establishment request, and the downlink message from the AMF was a service accept, which was sent as a protected message. However, the UE did not provide a response to the service accept message. According to the 3GPP standards, once the 5G-AKA is completed, the NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF's downlink message was sent as protected suggests that the encryption was applied as expected. However, the lack of response from the UE could indicate a potential issue in the communication process, such as a failure to properly decrypt or process the message, or a deliberate test condition. Without further information on why the UE did not respond, it is difficult to definitively conclude the security status. However, based on the available information, the UE's action of not responding could be seen as a failure to maintain secure communication as per the 3GPP standards, which require proper handling of protected messages. Therefore, the action taken by the UE appears to be insecure. Insecure
100	100	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 92 UE provided: No response The packet capture during the test using wireshark is: 0.4685640335083008 UE to AMF UplinkNASTransport, Registration complete 0.4687800407409668 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Insufficient user-plane resources for the PDU session) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "registration complete" message, followed by the AMF sending a "gmm status" message with a 5GMM Cause of 92, indicating "Insufficient user-plane resources for the PDU session." The downlink message from the AMF was sent as "Protected," suggesting that encryption was applied, which is consistent with the requirement that messages be encrypted after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE, however, did not provide a response to the "gmm status" message. According to the 3GPP standards, the UE should handle such status messages appropriately, potentially by taking corrective actions or notifying the user. The lack of response from the UE could indicate a failure to adhere to the expected behavior as per the standards, which might expose the UE to potential vulnerabilities or service disruptions. Therefore, while the initial encryption of the message exchange suggests a level of security, the UE's lack of response to the status message raises concerns about its compliance with the 3GPP standards and its ability to handle network-initiated messages securely. Based on this analysis, the UE's action in this scenario is deemed "Insecure."

101	101	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: No response The packet capture during the test using wireshark is: 4.873120069503784 UE to AMF SACK (Ack=7, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 4.873471021652222 AMF to UE SACK (Ack=9, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an uplink NAS transport message, followed by the AMF responding with a security mode command. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to this exchange, which is a prerequisite for secure communication. The security mode command from the AMF was sent as a protected message, indicating that it was integrity protected with a new security context, using the specified cipher and integrity algorithms (128-5G-EA3 and 128-5G-IA2, respectively). However, the UE did not provide a response to the security mode command. According to the 3GPP standards, after receiving a security mode command, the UE should respond with a security mode complete message to confirm the establishment of the security context. The absence of a response from the UE suggests a failure to complete the security procedure, which could leave the communication vulnerable to interception or tampering. Therefore, based on the 3GPP standards, the UE's lack of response indicates that the action taken 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request. Following this, the AMF responded with a security mode command, which was sent as a protected message. The security mode command utilized the 5G-EA0 (null) ciphering algorithm and the 5G-IA0 (null) integrity algorithm, with the security header indicating that the message was integrity protected with a new security context. However, the UE responded with a 5GMM status message indicating "Invalid mandatory information." This suggests that the UE did not accept the security mode command, likely due to the use of null algorithms for both ciphering and integrity protection, which do not provide actual encryption or integrity protection. According to the 3GPP 5G standards, the use of null algorithms is generally not secure for protecting NAS messages, as they do not offer confidentiality or integrity assurance. The UE's response of invalid mandatory information could indicate that it detected the lack of proper security measures and rejected the security mode command, which would be a secure action. However, if the UE was expected to proceed with communication under these conditions, it would be considered insecure. Given the context of the test and the UE's response, it appears that the UE acted securely by not accepting the insecure security mode command. Therefore, the action taken by the UE was "Secure."
103	103	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5199828147888184 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5202269554138184 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated communication by sending an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a deregistration request to the UE, which was integrity protected and ciphered, indicating that the message was secured according to the 5G security standards. However, the UE did not provide any response to the deregistration request. According to the 3GPP standards, the UE is expected to respond to such requests, especially when they are protected, to ensure proper session management and security compliance. The lack of response from the UE could indicate a potential issue in handling secure messages or a failure to comply with the expected protocol behavior. This non-compliance with the expected response protocol suggests a security vulnerability in the UE's handling of NAS messages, as it did not adhere to the standard procedure of acknowledging or responding to a protected deregistration request. Therefore, based on the observed interaction and the 3GPP standards, the action taken by the UE was insecure. Insecure

104	104	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5198929309844971 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5201320648193359 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (LADN not available) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated an uplink NAS transport message, specifically a PDU session establishment request, which was acknowledged by the AMF. Subsequently, the AMF sent a deregistration request to the UE, indicating that the UE was to be deregistered, possibly due to the unavailability of the Local Area Data Network (LADN). This downlink message from the AMF was protected, with the security header indicating that it was both integrity protected and ciphered. However, the UE did not provide any response to the deregistration request. According to the 3GPP standards, the integrity protection and ciphering of NAS messages are crucial for ensuring secure communication. The fact that the AMF's message was protected aligns with these security requirements. However, the lack of response from the UE could be a concern, as it might indicate an inability to process or respond to the deregistration request, which could be due to a security issue or a malfunction. Without a response, it is unclear if the UE properly handled the deregistration process, which is a critical aspect of maintaining secure and reliable network operations. Therefore, while the initial communication was secure, the absence of a response from the UE raises concerns about its compliance with the 3GPP security standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated communication by sending an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a configuration update command back to the UE. This downlink message was protected, as indicated by the security header being both integrity protected and ciphered. The UE then acknowledged this by sending a configuration update complete message back to the AMF. The sequence of messages suggests that the UE adhered to the security protocols outlined by the 3GPP standards, as the communication was encrypted and integrity protected, which are essential components of secure NAS communication in 5G networks. The completion of the 5G-AKA process prior to these exchanges ensured that the necessary security keys were established, allowing for the secure exchange of messages. Therefore, based on the adherence to these security measures, the actions taken by the UE can be considered 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the completion of the 5G Authentication and Key Agreement (5G-AKA) process, which is a prerequisite for secure communication. Following this, the UE sent a service request to the AMF, which responded with a Security Mode Command. This command was sent as a protected downlink message, utilizing the cipher algorithm 5G-EA4 and the integrity algorithm 128-5G-IA3, with a security header indicating integrity protection with a new security context. However, the UE responded with a Security Mode Reject message, citing a mismatch in UE security capabilities. This indicates that the UE detected a discrepancy between its security capabilities and the security requirements specified by the AMF. According to the 3GPP standards, the UE is expected to reject security mode commands if there is a mismatch in security capabilities, as this could potentially expose the UE to vulnerabilities or incompatibilities. By rejecting the security mode command, the UE adhered to the 3GPP standards, ensuring that it did not proceed with a potentially insecure configuration. Therefore, the action taken by the UE was secure, as it correctly identified and responded to a security capabilities mismatch, thereby maintaining the integrity and security of the communication. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated the communication by sending an "UplinkNASTransport" message with a "Registration complete" indication to the AMF. Subsequently, the AMF responded with a "DownlinkNASTransport" message containing a "Deregistration request" for UE termination, which was integrity protected and ciphered, indicating that the message was encrypted and authenticated. The UE then sent an "UplinkNASTransport" message with a "Deregistration accept" response, acknowledging the deregistration request. The sequence of messages suggests that the UE adhered to the 5G security protocols by ensuring that the communication was protected after the 5G-AKA process, which is a prerequisite for secure message exchange. The use of integrity protection and ciphering in the downlink message from the AMF indicates compliance with the 3GPP standards for secure communication. Therefore, based on the observed interaction and adherence to the 5G security standards, the actions taken by the UE can be considered secure. Secure

108	108	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.5200989246368408 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5204448699951172 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7219538688659668 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is essential for establishing a secure communication channel. Following this, the UE sent an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a configuration update command back to the UE, which was integrity protected with a new security context, indicating that the message was secured according to the 5G security standards. However, the UE responded with a 5GMM status message indicating that the message type was not compatible with the protocol state. This response suggests that the UE did not recognize or accept the configuration update command in its current protocol state, which could be due to a mismatch in expected message types or states. The fact that the UE flagged the message as incompatible rather than processing it without verification indicates that the UE adhered to protocol checks, which is a positive security measure. However, the inability to process a legitimate message due to protocol state issues could also suggest a potential flaw in handling state transitions or message expectations. Overall, while the UE's response shows adherence to protocol checks, the situation highlights a potential area for improvement in handling unexpected or out-of-sequence messages. Based on the 3GPP standards, the UE's action of rejecting an incompatible message type is a secure behavior, as it prevents the processing of potentially harmful or unexpected messages. Therefore, the UE's actions can be considered "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After the successful completion of the 5G Authentication and Key Agreement (5G-AKA), which is necessary for securing communications, the UE sent an "Uplink NAS Transport" message to the AMF, indicating a PDU session establishment request. In response, the AMF sent a "GMM Status" message back to the UE, which was protected, meaning it was encrypted as per the 5G security standards. The 5GMM cause code 98 indicates that the message type was not compatible with the protocol state, suggesting a potential issue with the message sequence or state management. The UE then responded with a "5GMM Status" message, acknowledging the incompatibility. According to the 3GPP standards, the UE's response to an unexpected or incompatible message should be to maintain the integrity and confidentiality of the communication, which it did by sending a status message indicating the protocol state issue. This behavior aligns with the security principles of the 5G standard, as the UE did not process the incompatible message further, thereby preventing any potential security breach. Therefore, the action taken by the UE was secure, as it adhered to the protocol's requirements for handling such situations. Secure

110	110	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 101 UE provided: No response The packet capture during the test using wireshark is: 0.5881869792938232 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originating) 0.5883810520172119 AMF to UE SACK (Ack=6, Arwnd=106429) , DownlinkNASTransport, 5GMM status (Message not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. After the successful completion of the 5G Authentication and Key Agreement (5G-AKA), the UE sent an uplink NAS message indicating "registration complete." Subsequently, the AMF responded with a downlink NAS message, specifically a "gmm status" message, which was sent as protected. The 5GMM Cause code 101 indicates that the message was not compatible with the protocol state. Notably, the UE did not provide any response to this message. According to the 3GPP standards, once the 5G-AKA is completed, all NAS messages should be encrypted and integrity protected. The fact that the AMF's message was protected aligns with this requirement. However, the UE's lack of response to the "gmm status" message could be interpreted as a security measure, as the message was deemed incompatible with the protocol state, potentially indicating an anomaly or an unexpected state. This non-response could be a deliberate action to avoid processing a message that might compromise the UE's security. Therefore, based on the 3GPP standards and the context of the test, the UE's action of not responding to an incompatible message can be considered secure, as it prevents potential exploitation or protocol misuse. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF responded with a security mode command, which was sent as a protected downlink message. The security mode command specified the use of the 5G-EA5 ciphering algorithm and the 5G-IA0 (null) integrity algorithm, with the security header indicating integrity protection with a new security context. However, the UE responded with a security mode reject message, citing a mismatch in UE security capabilities. This indicates that the UE detected a discrepancy between its supported security capabilities and those requested by the AMF. According to the 3GPP standards, the UE is expected to reject security configurations that do not align with its capabilities to prevent potential vulnerabilities. By rejecting the security mode command due to a capabilities mismatch, the UE adhered to the security protocols designed to protect against improper or insecure configurations. Therefore, the action taken by the UE was in line with the 5G security standards, ensuring that only compatible and secure configurations are accepted. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF responded with a Security Mode Command, which was sent as a protected downlink message using the cipher algorithm 5G-EA5 and the integrity algorithm 128-5G-IA2. The security header indicated that the message was integrity protected with a new security context. However, the UE responded with a Security Mode Reject message, citing a mismatch in UE security capabilities. This indicates that the UE detected a discrepancy between its security capabilities and the security requirements specified by the AMF. According to the 3GPP standards, the UE is expected to reject security mode commands if there is a mismatch in security capabilities to prevent potential vulnerabilities or misconfigurations. By rejecting the security mode command, the UE adhered to the security protocols designed to protect against improper or unsupported security configurations. Therefore, the action taken by the UE was in line with the 5G security standards, ensuring that only compatible and secure configurations are accepted. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, establishing a security context for subsequent communications. The UE then sent a service request to the AMF, which responded with a Security Mode Command. This command was sent as a protected message, utilizing the cipher algorithm 128-5G-EA1 and the integrity algorithm 128-5G-IA2, with a security header indicating integrity protection with a new security context. However, the UE responded with a Security Mode Reject message, citing an unspecified reason for rejection. According to the 3GPP standards, the UE's action to reject the security mode command can be considered secure if the UE detected any inconsistencies or potential security threats in the received message. The rejection indicates that the UE is cautious and adheres to the security protocols by not accepting potentially compromised or incorrect security parameters. Therefore, the UE's action aligns with the security measures outlined by 3GPP, ensuring that only valid and secure communications are accepted. Secure.
114	114	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Configuration update complete The packet capture during the test using wireshark is: 0.5208940505981445 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5215411186218262 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7234148979187012 UE to AMF UplinkNASTransport, Configuration update complete This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed to assess the security of the UE's actions. The process began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for ensuring that subsequent messages are encrypted and integrity protected. Following this, the UE sent an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a configuration update command back to the UE, which was protected with a security header indicating that it was both integrity protected and ciphered. The UE then acknowledged this command by sending a configuration update complete message back to the AMF. The use of integrity protection and ciphering in the downlink message from the AMF suggests adherence to the 3GPP standards for secure communication, as these measures are designed to protect against eavesdropping and tampering. Given that the 5G-AKA was completed successfully and the subsequent messages were protected, the actions taken by the UE appear to be secure according to the 3GPP standards. Therefore, based on the observed interaction and the security measures in place, the UE's communication can be considered "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request, followed by the AMF responding with a security mode command. The security mode command was sent as a protected message, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is a prerequisite for secure communication. The security mode command utilized the cipher algorithm 5G-EA4 and the integrity algorithm 128-5G-IA3, with the security header indicating that the message was integrity protected with a new security context. However, the UE responded with a 5GMM status message indicating "Invalid mandatory information." This response suggests that the UE encountered an issue processing the security mode command, potentially due to incorrect or unexpected information in the message. According to the 3GPP standards, the UE should be able to process the security mode command correctly if the 5G-AKA procedure is completed successfully and the security algorithms are supported. The UE's response of "Invalid mandatory information" indicates a failure to adhere to the expected protocol, which could expose the communication to security vulnerabilities. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario is considered insecure. Insecure

116	116	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00d2 Cipher Algorithm: 128-5G-EA2 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.480457067489624 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.48129701614379883 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is essential for establishing a secure communication channel. Following this, the UE sent an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a downlink NAS transport message containing a security mode command, which was protected and included parameters such as the ABBA value, cipher algorithm (128-5G-EA2), and integrity algorithm (128-5G-IA2). The security header indicated that the message was integrity protected with a new security context. However, the UE responded with a security mode reject message, citing an unspecified reason for rejection. According to the 3GPP standards, the UE's action to reject the security mode command can be considered secure if the UE detected any inconsistencies or potential security threats in the parameters or the context provided by the AMF. The rejection indicates that the UE is cautious and adheres to the security protocols by not accepting potentially insecure configurations. Therefore, based on the information provided and the UE's adherence to security protocols, the action taken by the UE appears to be secure. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an uplink NAS transport message, followed by the AMF responding with a security mode command. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to this exchange, which is a prerequisite for secure communication. The AMF's security mode command was sent as a protected message, indicating that it was both integrity protected and ciphered with a new security context, using the 5G-EA5 ciphering algorithm and the 128-5G-IA1 integrity algorithm. However, the UE did not provide a response to the security mode command. According to the 3GPP standards, the UE is expected to respond to the security mode command to establish a secure communication context. The lack of response from the UE suggests a failure to comply with the expected security procedures, potentially leaving the communication unprotected. This non-compliance with the 3GPP standards indicates that the UE's actions were insecure, as it did not complete the necessary steps to ensure the integrity and confidentiality of the communication. Therefore, based on the interaction and the standards, the UE's actions were "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated communication by sending an uplink NAS transport message, which included a PDU session establishment request. In response, the AMF sent a configuration update command to the UE, which was protected with integrity protection and ciphering, as indicated by the security header. The UE then acknowledged this command by sending a configuration update complete message back to the AMF. The use of integrity protection and ciphering in the downlink message from the AMF suggests that the communication was encrypted and protected, adhering to the security requirements outlined by the 3GPP standards for 5G networks. Since the 5G-AKA process was completed prior to these exchanges, it ensured that the subsequent messages were secure. The UE's actions, including the acknowledgment of the configuration update command, were consistent with secure communication practices as per the 5G standard. Therefore, based on the observed interaction and adherence to the 3GPP security protocols, the actions taken by the UE can be considered secure. Secure

119	119	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 1111 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA1 Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.5208361148834229 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5222671031951904 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.7242951393127441 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a security mode command to the UE, which was protected with a new security context, indicating that the message was integrity protected. The security mode command specified the use of the 5G-EA0 (null) ciphering algorithm and the 128-5G-IA1 integrity algorithm. However, the UE responded with a security mode reject message, citing an unspecified reason for rejection. According to the 3GPP standards, the UE's action to reject the security mode command can be considered secure if the UE detected any inconsistencies or potential security threats, such as the use of a null ciphering algorithm, which does not provide encryption. The rejection suggests that the UE prioritized maintaining a secure communication channel by not accepting potentially insecure parameters. Therefore, based on the 5G standard and the UE's cautious response to the security mode command, the action taken by the UE 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "registration complete" message, followed by the AMF sending a "deregistration accept" message. The 5G Authentication and Key Agreement (5G-AKA) process was completed prior to these exchanges, ensuring that subsequent messages should be encrypted as per the 3GPP standards. The packet capture indicates that the "deregistration accept" message from the AMF was sent as a protected message, which implies encryption was applied. However, the UE did not provide any response to the "deregistration accept" message. According to 3GPP standards, the UE should respond appropriately to such messages to maintain a secure communication channel. The lack of response from the UE could indicate a potential issue in handling the deregistration process securely. This absence of response might suggest a vulnerability or a non-compliance with the expected behavior outlined by the 3GPP standards, as the UE should ideally acknowledge or process the deregistration message to ensure a secure termination of the session. Therefore, based on the interaction and the UE's lack of response, the action taken by the UE appears to be insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed during the NAS communication phase. The UE sent an authentication response to the AMF, which is a standard procedure in the 5G-AKA (Authentication and Key Agreement) process. However, instead of proceeding with the authentication process, the AMF responded with a service reject message, citing a protocol error with an unspecified cause (5GMM Cause: 111). Notably, this downlink message from the AMF was sent in plain text, which is permissible at this stage since the 5G-AKA process had not been completed, and encryption had not yet been established. The UE did not provide any response to the service reject message. According to the 3GPP standards, the UE's actions were consistent with expected behavior, as it correctly sent an authentication response and did not proceed further without a successful authentication and encryption setup. The lack of response to the service reject message is also appropriate, given that the message indicated a protocol error. Therefore, the UE's actions can be considered secure, as it adhered to the 5G standard protocols by not engaging further without a completed authentication process. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an initial registration request to the AMF. The AMF responded with a service reject message, indicating that the UE identity could not be derived by the network, with a 5GMM Cause value of 9. Notably, the service reject message was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is a prerequisite for encrypting NAS messages. The UE did not provide any response to the service reject message. According to the 3GPP standards, the 5G-AKA procedure is essential for establishing a secure communication channel between the UE and the network. Since the 5G-AKA was not completed, the communication remained unencrypted, leaving it vulnerable to interception and potential security breaches. The lack of encryption and the UE's failure to respond to the service reject message suggest that the UE's actions were not aligned with the security protocols outlined by the 3GPP standards. Therefore, the UE's communication in this scenario can be considered insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. The UE initially sent an identity response to the AMF, which was followed by the AMF sending a security mode command back to the UE. Notably, the security mode command was sent as a protected message, indicating that it was integrity protected with a new security context, using the cipher algorithm 5G-EA4 and the integrity algorithm 128-5G-IA1. However, the UE responded with a security mode reject message, citing an unspecified reason for the rejection. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed first. In this scenario, the 5G-AKA was not completed, which means the security context was not fully established. The UE's rejection of the security mode command, given the incomplete 5G-AKA, suggests that the UE was cautious in not accepting a security context that might not have been fully secure. This cautious approach aligns with the 3GPP standards, which emphasize the importance of completing the authentication process before establishing a secure communication channel. Therefore, the UE's action to reject the security mode command without a completed 5G-AKA can be considered a secure response to ensure the integrity and confidentiality of its communications. 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 the test scenario, the User Equipment (UE) engaged in a Non-Access Stratum (NAS) communication with the Access and Mobility Management Function (AMF). The sequence of events began with the UE sending an identity response to the AMF. Subsequently, the AMF issued an identity request back to the UE, which was sent in plain text, requesting the Subscription Concealed Identifier (SUCI). The UE then responded with another identity response. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at this point, which is crucial for establishing a secure communication channel. According to the 3GPP standards, the 5G-AKA process must be completed to ensure that messages between the UE and the AMF are encrypted, thereby protecting sensitive information such as the SUCI. In this test, since the 5G-AKA was not completed, the communication was not encrypted, and the UE responded to a plain text identity request with an identity response. This action exposes the UE to potential security risks, as sensitive information could be intercepted or manipulated. Therefore, based on the 3GPP standards, the UE's action of responding to an unencrypted identity request without completing the 5G-AKA is considered insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was initiated by the UE sending an initial registration request. This uplink message was followed by a downlink message from the AMF, which was an authentication reject sent in plain text. The UE did not provide any response to this message. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to establish a secure communication channel, ensuring that subsequent messages are encrypted. In this scenario, the 5G-AKA was not completed, and the AMF's message was sent in plain text, which is a potential security risk. The UE's lack of response to the authentication reject could be interpreted as a cautious approach, as it did not proceed with any further actions without a secure channel being established. However, the fact that the UE did not respond at all could also indicate a lack of proper handling of such scenarios, which might be expected to trigger a security alert or a retry mechanism. Based on the 3GPP standards, the UE's action of not responding to an unencrypted authentication reject message can be seen as a secure approach, as it avoids engaging in potentially insecure communication. Therefore, the UE's behavior in this test scenario can be considered "Secure."
126	126	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5059909820556641 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5062329769134521 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7099969387054443 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a "registration complete" message, indicating that the initial registration process was successfully concluded. Following this, the AMF sent a "deregistration request" to the UE, which was integrity protected and ciphered, ensuring that the message was both authenticated and encrypted. The UE responded with a "deregistration accept" message, acknowledging the request from the AMF. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to these exchanges, which is a prerequisite for securing NAS messages. The use of integrity protection and encryption in the downlink message from the AMF aligns with the 3GPP standards for secure communication, as it ensures that the message is protected against tampering and eavesdropping. The UE's response to the deregistration request was appropriate and expected, as it adhered to the protocol by sending a deregistration accept message. Given that the communication was protected and the UE followed the standard procedures, the actions taken by the UE can be considered secure according to the 3GPP standards for 5G communication. Secure

127	127	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.03972792625427246 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response message to the AMF. Following this, the AMF sent a deregistration accept message back to the UE. Notably, the deregistration accept message was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed. According to the 3GPP standards, the 5G-AKA procedure is essential for establishing a secure communication channel, as it ensures that messages are encrypted and protected from potential interception or tampering. Since the 5G-AKA was not completed, the communication between the UE and the AMF was not encrypted, leaving it vulnerable to security threats. The UE did not provide any response to the deregistration accept message, which might indicate a lack of proper handling of unencrypted messages. Based on the 3GPP standards, the action taken by the UE in this scenario is considered insecure, as it engaged in communication without the necessary encryption safeguards in place. Insecure
128	128	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3031 RAND: 00000000000000000000000000000000 AUTN: 00000000000000000000000000000000 ngKSI_TSC: Mapped security context ngKSI_KSI: 1 UE provided: 5GMM status (Invalid mandatory information) The packet capture during the test using wireshark is: 0.03987288475036621 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04013490676879883 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.24352788925170898 UE to AMF UplinkNASTransport, 5GMM status (Invalid mandatory information) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) involves a sequence of NAS (Non-Access Stratum) messages. The UE initially sends an identity response to the AMF, which is a standard procedure in the NAS communication process. Following this, the AMF sends an authentication request to the UE. Notably, this authentication request is sent in plain text, which is unusual because, according to the 5G standard outlined by 3GPP, the 5G Authentication and Key Agreement (5G-AKA) procedure should be completed before any messages are encrypted. The AMF's use of a plain text message indicates that the security context has not been established yet. The UE responds with a 5GMM status message indicating "Invalid mandatory information," which suggests that the UE detected an anomaly or inconsistency in the received message, possibly due to the plain text format or the zeroed-out RAND and AUTN values. This response from the UE is consistent with the 5G standard, as it is expected to reject or flag any authentication requests that do not meet the security requirements. The UE's action to not proceed with the authentication process under these conditions demonstrates adherence to the security protocols defined by 3GPP, ensuring that it does not engage in potentially insecure communication. Therefore, based on the UE's response to the AMF's plain text authentication request, the UE's actions can be considered secure. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is crucial for establishing a secure communication channel. Following this, the UE sent an authentication response to the AMF, which then replied with a security mode command. This command was sent as a protected downlink message, indicating that the AMF intended to establish a secure communication context using the specified cipher and integrity algorithms. The cipher algorithm used was 5G-EA0 (null), which means no encryption was applied, while the integrity algorithm was 128-5G-IA2, ensuring message integrity. The security header indicated that the message was integrity protected with a new security context. However, the UE responded with a security mode reject message, citing an unspecified reason. This rejection suggests that the UE did not accept the security parameters proposed by the AMF, possibly due to the use of the null cipher algorithm, which does not provide encryption. According to the 3GPP standards, the UE's action to reject the security mode command can be considered secure, as it did not agree to a security context that lacked encryption, thereby preventing potential exposure of sensitive information. Therefore, the UE's decision to reject the security mode command aligns with maintaining a secure communication standard. Secure.

130	130	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3131 RAND: 35353535353535353535353535353535 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: Authentication failure (Non-5G authentication unacceptable) The packet capture during the test using wireshark is: 0.04801797866821289 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04822111129760742 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request 0.25036191940307617 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an authentication request. The authentication request was sent in plain text, which is permissible at this stage since the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The UE responded with an authentication failure message, indicating that the authentication method was "Non-5G authentication unacceptable." This response suggests that the UE detected an issue with the authentication request, possibly due to the use of an inappropriate or unsupported authentication method, or because the request did not adhere to the expected 5G security protocols. According to the 3GPP standards, the UE is expected to reject any authentication attempts that do not comply with the 5G security framework, which includes ensuring that the authentication method is appropriate and that the security context is correctly established. By rejecting the authentication request, the UE demonstrated adherence to the 5G security standards, as it did not proceed with an authentication process that could potentially compromise its security. Therefore, the action taken by the UE was in line with the 3GPP standards and can be considered secure. Secure
131	131	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 26 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00038909912109375 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Registration reject (Non-5G authentication unacceptable) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was initiated by the UE sending an initial registration request. The AMF responded with a registration reject message, citing a 5GMM Cause of 26, which corresponds to "Non-5G authentication unacceptable." Notably, this downlink message from the AMF was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed. The UE did not provide any response to the registration reject message. According to the 3GPP standards, the 5G-AKA procedure is crucial for establishing a secure communication channel, as it ensures that messages are encrypted and authenticated. Since the 5G-AKA was not completed, the communication remained unencrypted, leaving it vulnerable to interception and tampering. The UE's lack of response to the registration reject message is consistent with the standard, as it did not proceed with any further actions without a secure channel being established. However, the initial registration request was sent without the security context being established, which could be considered a security risk. Therefore, based on the 3GPP standards, the UE's action in this scenario can be deemed insecure due to the lack of encryption and authentication in the communication. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response message to the AMF. Following this, the AMF sent a service reject message back to the UE, with the 5GMM Cause code 99, indicating "Information element non-existent or not implemented." Notably, this downlink message from the AMF was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed. According to the 3GPP standards, for messages to be encrypted, the 5G-AKA must be completed to establish a secure context. Since the 5G-AKA was not completed, the communication remained unencrypted, leaving the UE's identity response potentially exposed to interception. The UE did not provide any further response after receiving the service reject message. Based on the 3GPP standards, the UE's action of sending an identity response before the completion of 5G-AKA, and thus without encryption, is considered insecure as it does not adhere to the security protocols designed to protect user identity and data. Therefore, the UE's communication in this scenario is deemed "Insecure."
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. The UE initially sent an identity response to the AMF, which was followed by an authentication request from the AMF. Notably, the authentication request was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is necessary for establishing a secure communication channel. The AMF's message included parameters such as ABBA, RAND, AUTN, and ngKSI values. The UE responded with an authentication failure message, indicating that the authentication method was "Non-5G authentication unacceptable." This response suggests that the UE detected an issue with the authentication request, possibly due to the lack of encryption or the use of non-standard parameters, and rejected it as per the 3GPP standards. The UE's action to reject the authentication request in the absence of a completed 5G-AKA process aligns with the security protocols outlined by 3GPP, which emphasize the importance of secure and encrypted communication. By refusing to proceed with an insecure authentication process, the UE demonstrated adherence to the security standards, ensuring that sensitive information was not exposed. Therefore, the action taken by the UE 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed during the NAS communication phase. The UE sent an identity response to the AMF, which was followed by a service reject message from the AMF. Notably, the service reject message was sent in plain text, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, as encryption of NAS messages is contingent upon the successful completion of 5G-AKA. The 5GMM Cause code of 3, which corresponds to "Illegal UE," suggests that the AMF rejected the service request due to the UE being considered unauthorized or unrecognized. Since the UE did not provide any further response after receiving the service reject message, it adhered to the expected behavior by not attempting to continue communication without proper authentication and encryption. According to the 3GPP standards, the UE should not engage in further communication if the 5G-AKA is not completed, as this ensures that sensitive information is not transmitted in an unprotected manner. Therefore, the UE's action of ceasing communication upon receiving the service reject message aligns with the security protocols outlined by 3GPP, indicating that the UE acted securely in this scenario. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. The AMF responded with a security mode command, which was sent as a protected message. However, the protection was minimal, using the 5G-EA0 (null) cipher algorithm and the 5G-IA0 (null) integrity algorithm, indicating no encryption or integrity protection was applied. The security header indicated that the message was integrity protected with a new security context, but without completing the 5G Authentication and Key Agreement (5G-AKA), the security context was not fully established. Consequently, the UE responded with a security mode reject message, citing an unspecified reason for rejection. This action by the UE suggests that it did not accept the security mode command due to the lack of proper encryption and integrity protection, which aligns with the 3GPP standards that require a secure context before proceeding with encrypted communications. By rejecting the security mode command under these conditions, the UE demonstrated adherence to security protocols, ensuring that communication would not proceed without adequate protection. Therefore, the action taken by the UE 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, the interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) involved a sequence of NAS messages. The UE first sent an identity response to the AMF, which then replied with a security mode command. This command was sent as a protected message, indicating that it was integrity protected with a new security context, but not encrypted, as the 5G-AKA procedure had not been completed. The security mode command specified the use of the 5G-EA0 ciphering algorithm, which is essentially a null algorithm, meaning no encryption, and the 128-5G-IA3 integrity algorithm. The UE responded with a security mode reject message, citing an unspecified reason for rejection. According to the 3GPP 5G standards, the UE's action to reject the security mode command can be considered secure. This is because the 5G-AKA procedure, which is essential for establishing a secure context, was not completed, and the use of the 5G-EA0 null ciphering algorithm would not provide encryption for the messages. By rejecting the security mode command, the UE avoided proceeding with a potentially insecure communication setup. Therefore, the UE's decision to reject the security mode command aligns with maintaining security standards by not accepting a configuration that lacks proper encryption. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was focused on the authentication process. Initially, the UE sent an authentication response to the AMF, which was followed by the AMF sending an authentication request back to the UE. Notably, the downlink message from the AMF was sent in plain text, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, as encryption of messages is contingent upon the successful completion of this procedure. The UE then responded with another authentication response. According to the 3GPP standards, the 5G-AKA procedure is crucial for establishing a secure communication channel by ensuring mutual authentication and deriving encryption keys. The fact that the AMF sent an authentication request in plain text suggests that the security context was not established, leaving the communication vulnerable to interception and manipulation. The UE's action of responding to a plain text authentication request without the completion of 5G-AKA indicates a potential security flaw, as it should ideally wait for a secure context to be established before proceeding with sensitive exchanges. Therefore, based on the 3GPP standards and the observed interaction, the UE's actions were insecure. Insecure

138	138	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.5089499950408936 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5091559886932373 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) 0.7129359245300293 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated the communication by sending a "registration complete" message to the AMF, indicating that it had successfully registered with the network. Subsequently, the AMF sent a "deregistration request" to the UE, which was integrity protected and ciphered, ensuring that the message was both authenticated and encrypted. The UE responded with a "deregistration accept" message, acknowledging the request from the AMF. The use of integrity protection and encryption in the downlink message from the AMF suggests adherence to the 3GPP standards for secure communication, as these measures are designed to protect against tampering and eavesdropping. The UE's response to the deregistration request, after receiving a protected message, indicates that it followed the expected protocol for secure communication. Given that the 5G-AKA process was completed, which is a prerequisite for secure message exchange, and the subsequent messages were protected, the actions taken by the UE appear to be in line with the security requirements outlined by the 3GPP standards. Therefore, the communication between the UE and the AMF can be considered secure. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. Following this, the AMF responded with an authentication request, which was sent in plain text. The authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI values. However, the UE responded with a 5GMM status indicating "Invalid mandatory information." This response suggests that the UE detected an issue with the received authentication request, possibly due to the plain text nature of the message or incorrect parameters, and flagged it as invalid. According to the 3GPP standards, the 5G-AKA procedure must be completed to establish a secure context for encrypting messages. Since the 5G-AKA was not completed, the UE's response to reject the authentication request due to invalid information aligns with the security protocols designed to prevent unauthorized access or potential security breaches. The UE's action to not proceed with the authentication process without a valid and secure context indicates adherence to the 5G security standards. Therefore, the UE's behavior in this scenario can be considered secure, as it did not accept potentially insecure communication. 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 User Equipment (UE) initiated a registration process by sending an initial registration request to the Access and Mobility Management Function (AMF). The AMF responded with an authentication request, which was sent in plain text, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The UE then responded with a deregistration request, indicating that it chose to terminate the registration process. According to the 3GPP standards, the 5G-AKA procedure is crucial for establishing a secure communication channel, as it ensures mutual authentication and the derivation of encryption keys for subsequent messages. Since the authentication request was sent in plain text and the 5G-AKA was not completed, the communication was not secure. The UE's decision to deregister can be seen as a precautionary measure to avoid proceeding with an insecure connection. However, the initial interaction, where sensitive information could potentially be exposed due to the lack of encryption, indicates a vulnerability. Therefore, based on the 3GPP standards, the UE's communication in this scenario was insecure. Insecure
141	141	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.17494893074035645 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.17513012886047363 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response following the initial NAS communication steps. Subsequently, the AMF sent an authentication reject message back to the UE. Notably, this downlink message from the AMF was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is a prerequisite for encrypting messages between the UE and the AMF. The UE did not provide any response to the authentication reject message. According to the 3GPP standards, the UE should not proceed with any further communication or actions if it receives an authentication reject message, as this indicates a failure in the authentication process. The lack of response from the UE aligns with the expected behavior, as it should not attempt to establish a secure connection or proceed with any further NAS procedures without successful authentication. Therefore, the UE's action of not responding to the authentication reject message is consistent with maintaining security as per the 3GPP standards, as it prevents any potential unauthorized access or communication. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was focused on the authentication process. Initially, the UE sent an authentication response to the AMF, which was followed by an authentication request from the AMF. Notably, the AMF sent this request as a plain message, which is unusual because, according to the 3GPP standards, messages should be encrypted after the 5G Authentication and Key Agreement (5G-AKA) procedure is completed. The UE responded with an authentication failure message, indicating that the non-5G authentication was unacceptable. This response suggests that the UE correctly identified the issue with the authentication request being sent in plain text and the lack of completion of the 5G-AKA process, which is necessary for secure communication. By rejecting the authentication request, the UE adhered to the security protocols outlined by the 3GPP standards, which emphasize the importance of completing the 5G-AKA process before proceeding with encrypted communication. Therefore, the UE's action was in line with maintaining the security integrity of the communication process. Secure.
143	143	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.5046439170837402 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request, UplinkNASTransport, Deregistration request (UE originating) 0.5048840045928955 AMF to UE SACK (Ack=7, Arwnd=106334) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is a prerequisite for ensuring that subsequent messages are encrypted and integrity protected. Following this, the UE sent an uplink NAS message indicating "registration complete" to the AMF. In response, the AMF sent a downlink NAS message with a "deregistration request," which was integrity protected and ciphered, indicating that the message was secured according to the 5G standards. However, the UE did not provide any response to this deregistration request. The lack of response from the UE could be interpreted in different ways: it might be due to a security feature where the UE does not respond to unexpected or suspicious messages, or it could be a failure in the UE's handling of the deregistration request. According to the 3GPP standards, the UE should be able to handle such messages securely, either by responding appropriately or by taking measures to protect itself from potential security threats. Given that the UE did not respond, it suggests a potential issue in its handling of the deregistration request, which could be seen as a security vulnerability. Therefore, based on the interaction and the lack of response from the UE, the action taken by the UE appears to be insecure according to the 5G standard outlined by 3GPP. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed to assess the security of the UE's actions. The process began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for ensuring that subsequent NAS (Non-Access Stratum) messages are encrypted and integrity protected. Following this, the UE sent an uplink NAS message indicating "registration complete" to the AMF. In response, the AMF sent a downlink NAS message, specifically a "configuration update command," which was protected with a security header indicating that it was both integrity protected and ciphered. The UE then responded with an uplink NAS message, "configuration update complete," confirming the receipt and processing of the configuration update command. The packet capture from Wireshark corroborates this sequence of events, showing that the messages were exchanged as expected. Given that the 5G-AKA was completed successfully, and the subsequent messages were protected as per the 3GPP standards, the UE's actions adhered to the security protocols required for secure communication. Therefore, based on the outlined interaction and adherence to the 5G security standards, the UE's actions can be considered 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was focused on the NAS (Non-Access Stratum) security procedures. Initially, the 5G Authentication and Key Agreement (5G-AKA) was completed, which is a prerequisite for establishing a secure communication channel. The UE then sent a "security mode complete" message to the AMF, indicating that it accepted the security parameters proposed by the AMF. However, the AMF subsequently sent a "security mode command" back to the UE, which was protected, indicating that the message was integrity protected with a new security context. The ciphering algorithm used was 5G-EA0 (null), meaning no encryption was applied, while the integrity algorithm was 128-5G-IA2, ensuring message integrity. The UE responded again with a "security mode complete" message. The use of the null ciphering algorithm (5G-EA0) suggests that the messages were not encrypted, which is generally not secure for protecting the confidentiality of the communication. However, the integrity protection was applied, which ensures that the messages were not tampered with during transmission. According to the 3GPP standards, while integrity protection is crucial, the lack of encryption (ciphering) could expose the communication to eavesdropping, making the action taken by the UE insecure in terms of confidentiality. Therefore, based on the 5G standard, the UE's communication in this scenario is considered "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After the successful completion of the 5G Authentication and Key Agreement (5G-AKA), which is crucial for establishing a secure communication channel, the UE sent a "security mode complete" message to the AMF. This indicates that the UE accepted the security parameters and was ready to proceed with secure communication. However, the subsequent message from the AMF was a "deregistration accept," which was sent as a protected message, indicating that it was encrypted. The UE did not respond to this message. The lack of response from the UE could be interpreted in different ways, but given that the deregistration accept message was protected, it suggests that the communication was encrypted and followed the security protocols as per the 3GPP standards. The UE's action of not responding could be due to the test setup or a specific test condition, but it does not inherently indicate a security flaw in the UE's behavior. Therefore, based on the information provided and the adherence to the 5G security protocols, the UE's actions appear to be secure. Secure
147	147	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected with new security context (3) UE provided: 5GMM status (Message type not compatible with the protocol state) The packet capture during the test using wireshark is: 0.15987586975097656 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16038084030151367 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.3645758628845215 UE to AMF UplinkNASTransport, 5GMM status (Message type not compatible with the protocol state) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "security mode complete" message to the AMF, indicating that it had successfully established a security context. Subsequently, the AMF sent a "configuration update command" to the UE, which was protected with integrity using the new security context. However, the UE responded with a "5GMM status" message indicating that the message type was not compatible with the protocol state. This suggests that the UE detected an inconsistency or unexpected message type, which could be a result of a protocol misalignment or an intentional security test to assess the UE's response to unexpected messages. According to the 3GPP standards, the UE should maintain the integrity and confidentiality of messages and respond appropriately to any anomalies. The UE's response to the configuration update command by sending a 5GMM status message indicates that it recognized a potential issue and acted to maintain protocol integrity. This behavior aligns with the security principles outlined by 3GPP, as the UE did not blindly accept the message but instead flagged it as incompatible, which is a secure response to an unexpected or potentially malicious message. Therefore, based on the interaction and the UE's adherence to protocol integrity, the action taken by the UE was secure. Secure

148	148	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: Deregistration accept (UE terminated) The packet capture during the test using wireshark is: 0.11970210075378418 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.11996603012084961 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Congestion) 0.3268871307373047 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for secure communication. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it had successfully established a secure communication mode. The AMF then sent a "deregistration request" to the UE, which was integrity protected and ciphered, ensuring that the message was both authenticated and encrypted. The UE responded with a "deregistration accept" message, acknowledging the request. The packet capture shows that the messages were exchanged with appropriate security headers, indicating that the communication was protected as per the 3GPP standards. The UE's actions, including the acknowledgment of the deregistration request, were consistent with the expected behavior in a secure communication scenario. Given that the 5G-AKA was completed and the messages were protected, the UE's actions adhered to the security protocols outlined by 3GPP, ensuring the integrity and confidentiality of the communication. Therefore, the action taken by the UE was secure. Secure
149	149	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 3000 Cipher Algorithm: 5G-EA7 Integrity Algorithm: 128-5G-IA2 Security header: Integrity protected (1) UE provided: Security mode complete The packet capture during the test using wireshark is: 0.16007494926452637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16037607192993164 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.364534854888916 UE to AMF UplinkNASTransport, Security mode complete, Registration request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was focused on the NAS (Non-Access Stratum) security procedures. Initially, the 5G Authentication and Key Agreement (5G-AKA) was completed, which is a prerequisite for secure communication. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters, including the ciphering and integrity protection algorithms. However, the AMF then sent a "security mode command" back to the UE, which is unusual because this command is typically sent before the "security mode complete" message. The packet capture shows that the downlink message from the AMF was protected, and the security header was integrity protected, which suggests that the communication was encrypted and integrity-protected as per the 5G standards. The UE's response to the AMF's command was another "security mode complete" message, which indicates that the UE continued to operate under the assumption that the security context was valid. Based on the 3GPP standards, the UE's actions appear to be secure because it adhered to the security procedures by completing the 5G-AKA and responding with integrity-protected messages. However, the unusual sequence of messages from the AMF could indicate a potential issue in the test setup rather than a flaw in the UE's security handling. Therefore, considering the UE's adherence to the security protocols, the action taken by the UE was secure. Secure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "security mode complete" message, indicating that it had successfully established a secure communication mode with the AMF. Subsequently, the AMF sent a "deregistration request" to the UE, which was integrity protected and ciphered, ensuring that the message was both authenticated and encrypted. The UE responded with a "deregistration accept" message, acknowledging the request. The packet capture shows that the messages were exchanged with appropriate security headers, indicating that the communication was protected as per the 3GPP standards. The UE's actions, including the acceptance of the deregistration request, were consistent with the expected behavior in a secure communication scenario, as the messages were integrity protected and ciphered, ensuring confidentiality and authenticity. Therefore, based on the 5G standard outlined by 3GPP, the UE's actions can be considered secure. Secure
151	151	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00026297569274902344 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. Following this, the AMF responded with an identity request, specifically asking for the Globally Unique Temporary Identifier (GUTI) from the UE. Notably, this identity request was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The UE did not provide a response to the identity request. According to the 3GPP standards, the 5G-AKA procedure is crucial for establishing a secure communication channel, as it ensures that subsequent messages are encrypted and protected from potential interception or tampering. The UE's lack of response to the identity request in plain text can be considered a secure action, as responding could have exposed sensitive information without the protection of encryption. By not responding, the UE avoided the risk of transmitting potentially sensitive identity information over an unprotected channel, adhering to the security principles outlined by 3GPP. Therefore, the UE's action in this scenario was "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an initial registration request to the AMF. Subsequently, the AMF responded with a configuration update command. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at the time of this interaction, which is crucial for establishing a secure communication channel. The downlink message from the AMF was sent as "Protected," but the security header was marked as "Unknown," and the UE did not provide any response to the configuration update command. According to the 3GPP standards, for messages to be encrypted and secure, the 5G-AKA procedure must be completed to establish the necessary security context. Since the 5G-AKA was not completed, the UE's communication was not encrypted, leaving it vulnerable to potential security threats. The lack of a response from the UE could indicate an issue with processing the message or a deliberate action to avoid processing an unprotected message. However, the absence of encryption due to the incomplete 5G-AKA process suggests that the UE's actions were insecure according to the 5G standard. Therefore, the communication between the UE and the AMF in this scenario was "Insecure."
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. Following this, the AMF responded with a security mode command, which was sent as a protected downlink message. The security mode command was intended to establish a security context, using the cipher algorithm 128-5G-EA3 and the integrity algorithm 5G-IA0 (null). The security header indicated that the message was integrity protected with a new security context. However, the UE responded with an uplink message indicating a 5GMM status of "Invalid mandatory information." This suggests that the UE did not properly process the security mode command, possibly due to the incomplete 5G-AKA procedure, which is essential for establishing a secure communication channel. The 5G-AKA procedure must be completed to ensure that messages are encrypted and integrity protected according to the 3GPP standards. Since the UE's response indicated an issue with mandatory information and the 5G-AKA was not completed, the UE's actions in this scenario were insecure. The lack of a completed authentication and key agreement process means that the communication could be vulnerable to interception or manipulation. Therefore, based on the 3GPP standards, the UE's actions were "Insecure."

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an initial registration request to the AMF. Following this, the AMF responded with a configuration update command, which was sent as a protected message with a security header indicating that it was both integrity protected and ciphered. However, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at the time of this interaction. According to the 3GPP standards, for messages to be securely encrypted, the 5G-AKA process must be completed to establish the necessary security context. Since the 5G-AKA was not completed, the UE did not have the security context required to decrypt or verify the integrity of the configuration update command. Consequently, the UE did not respond to the AMF's message. This lack of response suggests that the UE did not process the message, which aligns with the expected behavior when the security context is not established. Therefore, the UE's action of not responding to a message that it could not securely process is consistent with maintaining security as per the 3GPP standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. This uplink message was intended to initiate the registration process with the network. However, the AMF, which was under test control, responded with a deregistration accept message, effectively terminating the registration process. Notably, this downlink message from the AMF was sent as a protected message, but the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at this point. According to the 3GPP standards, the 5G-AKA procedure is essential for establishing a secure communication channel, as it ensures that messages are encrypted and integrity-protected. Since the 5G-AKA was not completed, the UE's communication was not secured by the necessary cryptographic protections. Furthermore, the UE did not provide any response to the deregistration accept message, which could indicate a lack of proper handling of unexpected or potentially malicious messages. Based on this interaction, the UE's actions were insecure because it engaged in communication without the completion of the 5G-AKA, leaving it vulnerable to potential security threats. Insecure

156	156	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Integrity protected with new security context (3) UE provided: Security mode reject (Security mode rejected, unspecified) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007860660552978516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.2037971019744873 UE to AMF UplinkNASTransport, Security mode reject (Security mode rejected, unspecified) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. Following this, the AMF responded with a security mode command, which was sent as a protected message. However, the protection was minimal, using the 5G-EA0 (null) cipher algorithm and the 5G-IA0 (null) integrity algorithm, indicating no encryption or integrity protection was applied. The security header indicated that the message was integrity protected with a new security context. The UE responded with a security mode reject message, citing an unspecified reason for rejection. This sequence of events suggests that the UE did not proceed with the security mode command due to the lack of proper encryption and integrity protection, as the 5G-AKA (Authentication and Key Agreement) procedure was not completed. According to the 3GPP 5G standards, the UE is expected to reject security mode commands that do not meet the required security criteria, such as proper encryption and integrity protection. By rejecting the security mode command under these circumstances, the UE adhered to the security protocols outlined by the 3GPP, ensuring that communication would not proceed without adequate security measures in place. Therefore, the action taken by the UE 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. This uplink message was followed by a downlink message from the AMF, which was a deregistration request. Notably, the deregistration request was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered. However, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at this point, which is a prerequisite for establishing a secure communication channel. The UE did not respond to the deregistration request. According to the 3GPP standards, the 5G-AKA procedure is essential for ensuring that messages are encrypted and integrity protected, thereby securing the communication. Since the 5G-AKA was not completed, the UE's communication was not fully secure, as it did not have the necessary security context established to verify the integrity and confidentiality of the messages. The lack of response from the UE could be seen as a cautious approach, but without the completion of 5G-AKA, the communication cannot be considered secure. Therefore, based on the 3GPP standards, the action taken by the UE was insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. The AMF's request was sent in plain text, asking for the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to ensure that messages between the UE and the AMF are encrypted, thereby securing the communication. In this scenario, since the 5G-AKA was not completed, the communication was not encrypted, and the AMF's identity request was sent in plain text. The UE's lack of response to the plain text identity request can be considered a secure action, as it avoided transmitting sensitive information without encryption. This behavior aligns with the security principles of the 5G standard, which emphasize the protection of user identity and information. Therefore, the UE's action in not responding to the plain text request was secure, as it prevented potential exposure of sensitive information. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response message to the AMF. Following this, the AMF sent a GMM status message back to the UE, indicating that roaming is not allowed in the current tracking area. Notably, this downlink message from the AMF was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed yet. According to the 3GPP standards, the 5G-AKA procedure is essential for establishing a secure communication channel, as it facilitates mutual authentication and the derivation of encryption keys. Since the 5G-AKA was not completed, the messages exchanged between the UE and the AMF were not encrypted, leaving the communication vulnerable to interception and potential tampering. The UE did not provide any response to the GMM status message, which could be interpreted as a lack of action to secure the communication. Based on the 3GPP standards, the UE's action in this scenario is considered insecure because the communication was not encrypted, and the UE did not take steps to ensure the security of the interaction. Therefore, the communication between the UE and the AMF was "Insecure."

160	160	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.038893938064575195 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039427995681762695 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response message to the AMF. Subsequently, the AMF sent a configuration update command back to the UE. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at the time of this interaction. As a result, the downlink message from the AMF was sent as a plain NAS message, without encryption, as indicated by the security header being set to "Plain NAS message (0)." The UE did not provide a response to this configuration update command. According to the 3GPP standards, NAS messages should be encrypted to ensure secure communication between the UE and the network, but this encryption can only occur after the successful completion of the 5G-AKA procedure. Since the 5G-AKA was not completed, the messages remained unencrypted, which is a security vulnerability. The UE's lack of response to the plain configuration update command suggests that it did not proceed with processing an unencrypted message, which aligns with secure behavior by not accepting potentially insecure communications. Therefore, based on the 3GPP standards, the UE's action of not responding to an unencrypted message is considered secure behavior in this context. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response message to the AMF. Following this, the AMF sent a deregistration accept message back to the UE. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at the time of this interaction. The packet capture indicates that the downlink message from the AMF was sent as "Protected," which implies that it was encrypted. However, for messages to be encrypted according to the 5G standard, the 5G-AKA procedure must be completed to establish security keys. Since the 5G-AKA was not completed, the UE's response to the deregistration accept message was absent, which could suggest that the UE did not process the message due to the lack of established security context. According to the 3GPP standards, the UE should not accept or process messages that are protected without a completed 5G-AKA, as this would mean the security context is not properly established. Therefore, the UE's lack of response to the deregistration accept message, given the incomplete 5G-AKA, aligns with secure behavior as per the 3GPP standards, ensuring that it does not process potentially insecure messages. 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 the test scenario, the User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). The UE sent an identity response message to the AMF, which subsequently replied with a service accept message. Notably, the service accept message from the AMF was sent as a protected message, indicating that it was encrypted. However, the 5G Authentication and Key Agreement (5G-AKA) procedure, which is essential for establishing a secure communication channel, had not been completed at the time of this interaction. According to the 3GPP standards, the 5G-AKA procedure must be completed before any NAS messages can be securely encrypted and protected. Since the 5G-AKA was not completed, the UE's identity response message was sent without the assurance of encryption, leaving it vulnerable to interception and potential exploitation. The lack of a secure channel at this stage of communication suggests that the UE's actions were not in compliance with the security protocols outlined by 3GPP for 5G networks. Therefore, the UE's communication in this scenario was insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response message to the AMF. Following this, the AMF sent a deregistration request to the UE, which was integrity protected and ciphered, indicating that the message was secured at the NAS layer. However, it is important to note that the 5G Authentication and Key Agreement (5G-AKA) procedure was not completed prior to this exchange. According to the 3GPP standards, the 5G-AKA procedure is essential for establishing a secure communication channel, as it ensures mutual authentication and the derivation of security keys for protecting NAS messages. Since the 5G-AKA was not completed, the security context necessary for encrypting and protecting the messages was not properly established. Consequently, the UE's lack of response to the deregistration request could be seen as a failure to handle the situation securely, as it did not verify the authenticity of the message due to the absence of a completed 5G-AKA process. Therefore, the UE's action in this scenario can be considered insecure, as it did not adhere to the security protocols outlined by the 3GPP standards for 5G communication. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. The UE initially sent an identity response to the AMF, which was followed by a security mode command from the AMF. Notably, the security mode command was sent as a protected message, indicating that it was integrity protected with a new security context, using the 5G-EA4 cipher algorithm and the 128-5G-IA1 integrity algorithm. However, the UE responded with a security mode reject message, citing an unspecified reason for the rejection. According to the 3GPP 5G standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed first. In this scenario, the 5G-AKA was not completed, which means the security context was not fully established. The UE's rejection of the security mode command, given the incomplete 5G-AKA, suggests that the UE was cautious about proceeding with a potentially insecure communication setup. This action aligns with the 5G security standards, which emphasize the importance of completing the authentication process before establishing a secure communication channel. Therefore, the UE's decision to reject the security mode command without a completed 5G-AKA was a secure action, as it prevented the establishment of a potentially insecure connection. 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 interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. Initially, the UE sent an identity response to the AMF, which was followed by the AMF sending a security mode command back to the UE. Notably, the security mode command was sent as a plain NAS message, indicating that encryption was not applied. The ciphering algorithm specified was 128-5G-EA2, but the integrity algorithm was set to 5G-IA0, which is a null algorithm, meaning no integrity protection was applied. The security header was also marked as a plain NAS message, further confirming the lack of encryption. Subsequently, the UE sent a deregistration request, which was UE-originated. According to the 5G standard outlined by 3GPP, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed, which was not the case here. The absence of encryption and integrity protection in the communication between the UE and AMF, especially when sensitive operations like security mode command and deregistration are involved, indicates a lack of adherence to the security protocols expected in 5G communication. Therefore, based on the 5G standard, the actions taken by the UE in this scenario were insecure, as the communication was not protected against potential interception or tampering. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. The UE sent an authentication response to the AMF, which is a part of the 5G Authentication and Key Agreement (5G-AKA) process. However, the 5G-AKA was not completed, as indicated in the test summary. Following this, the AMF sent a configuration update command to the UE, which was integrity protected but not encrypted, as the security header indicates. The UE did not provide any response to this command. According to the 3GPP standards, for messages to be encrypted, the 5G-AKA process must be completed to establish security keys. Since the 5G-AKA was not completed, the communication was not encrypted, which is a deviation from the expected secure communication protocol. The lack of encryption and the absence of a response from the UE suggest that the UE did not proceed with the configuration update command, possibly due to the incomplete security setup. This behavior aligns with the security expectations, as the UE should not process potentially insecure messages. Therefore, the UE's action of not responding to the configuration update command without completed 5G-AKA is considered secure. Secure

167	167	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.07818889617919922 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication response 0.07842707633972168 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response, followed by the AMF sending an identity request. The identity request from the AMF was sent in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to ensure that messages are encrypted, thereby protecting sensitive information such as the IMEISV. Since the 5G-AKA was not completed, the communication was not encrypted, and the AMF's request for the IMEISV was sent in plain text, which could potentially expose the UE to security risks if it had responded. The UE's lack of response to the identity request in plain text can be considered a secure action, as it avoided transmitting sensitive information without encryption. This behavior aligns with the security principles of minimizing exposure of sensitive data when encryption is not in place. Therefore, the UE's action in this scenario was "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 the test scenario, the User Equipment (UE) engaged in a sequence of NAS communications with the Access and Mobility Management Function (AMF). Initially, the UE sent an authentication response to the AMF, which is a part of the 5G Authentication and Key Agreement (5G-AKA) process. However, the 5G-AKA was not completed, as indicated in the test summary. Subsequently, the AMF sent a service accept message to the UE, which was protected, suggesting that some level of security was applied to this message. Following this, the UE sent a deregistration request, indicating that it intended to disconnect from the network. According to the 3GPP standards, for messages to be encrypted and secure, the 5G-AKA process must be completed to establish security keys. Since the 5G-AKA was not completed, the UE's communication, particularly the deregistration request, was likely not encrypted, leaving it potentially vulnerable to interception or tampering. The lack of completion of the 5G-AKA process before sending sensitive messages like the deregistration request suggests that the UE's actions were not fully secure according to the 5G standard. Therefore, the communication can be considered "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response to the AMF. Following this, the AMF sent a GMM status message back to the UE, which was transmitted in plain text. The 5GMM Cause code 26 indicates "Non-5G authentication unacceptable," suggesting that the AMF found the authentication response from the UE to be invalid or not meeting the expected criteria for 5G authentication. The UE did not provide any response to this message. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed successfully. Since the 5G-AKA was not completed, the communication remained unencrypted, which is a potential security risk. The UE's lack of response to the plain text GMM status message could be seen as a failure to handle the situation securely, as it did not attempt to reinitiate a secure authentication process or provide any corrective action. Therefore, based on the 3GPP standards and the observed behavior, the UE's actions in this scenario were insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. The UE sent an authentication response to the AMF, which is a part of the 5G Authentication and Key Agreement (5G-AKA) process. However, before the 5G-AKA could be completed, the AMF sent a deregistration request to the UE. This deregistration request was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered. Despite this protection, the UE did not provide any response to the deregistration request. According to the 3GPP standards, for messages to be encrypted, the 5G-AKA process must be completed, which was not the case here. The fact that the UE did not respond to the deregistration request could be seen as a security measure, as it did not engage further without a completed authentication process. However, the lack of response could also indicate a failure to handle unexpected or potentially malicious messages appropriately. Given that the 5G-AKA was not completed, and the UE did not respond to a protected message, the UE's action could be considered insecure as it did not follow through with the expected protocol behavior. Therefore, based on the 3GPP standards and the incomplete authentication process, the UE's communication in this scenario is deemed "Insecure."

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "security mode complete" message, indicating that it had accepted the security parameters established by the network. Subsequently, the AMF sent an "identity request" message to the UE, requesting the International Mobile Equipment Identity Software Version (IMEISV). Notably, this identity request was sent in plain text, which is a critical point of concern. According to the 3GPP standards, once the 5G-AKA process is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The UE, however, did not respond to the identity request, which could be interpreted as a refusal to transmit sensitive information over an unencrypted channel. This lack of response from the UE can be seen as a security-conscious action, adhering to the 3GPP standards that emphasize the importance of encrypted communication post-authentication. Therefore, the UE's decision not to respond to an unencrypted identity request aligns with secure communication practices as outlined by the 3GPP standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters and was ready for secure communication. However, the subsequent message from the AMF was an "identity request" sent in plain text, requesting the Globally Unique Temporary Identifier (GUTI) from the UE. The UE did not respond to this request. According to the 3GPP standards, once the 5G-AKA process is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The AMF's decision to send an identity request in plain text after the security mode was completed is a deviation from this standard, potentially exposing sensitive information. The UE's lack of response to the plain text identity request can be interpreted as a security measure, as responding to an unencrypted request could compromise the UE's identity. Therefore, the UE's action of not responding to the plain text identity request aligns with the 3GPP security standards, as it avoids transmitting sensitive information over an insecure channel. Secure

173	173	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent service reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: service reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 111 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.15993309020996094 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16013097763061523 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Service reject (Protocol error, unspecified) 0.3612639904022217 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with secure communication. However, the AMF responded with a "service reject" message, citing a protocol error with an unspecified cause (5GMM Cause: 111). Notably, this downlink message from the AMF was sent in plain text, which is unusual given that the 5G-AKA process had been completed, suggesting that encryption should have been in place. Subsequently, the UE sent a "deregistration request" to the AMF, indicating its intention to disconnect from the network. The UE's decision to deregister following the receipt of an unencrypted service reject message suggests that it recognized a potential security issue and took action to protect itself by terminating the session. According to the 3GPP standards, the UE should expect encrypted messages post-5G-AKA completion, and the receipt of a plain text message could be interpreted as a security anomaly. Therefore, the UE's action to deregister can be considered a secure response to an unexpected and potentially insecure situation. Secure.
174	174	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: c2ada16de5afa04c9abbf0b2aba327aa AUTN: 3030303030303000ee55922b5d550000 ngKSI_TSC: Native security context ngKSI_KSI: 3 UE provided: No response The packet capture during the test using wireshark is: 0.15995287895202637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16016292572021484 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After completing the 5G Authentication and Key Agreement (5G-AKA) process, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with secure communication. However, the subsequent message from the AMF was an "authentication request" sent in plain text, which is unusual because, according to the 3GPP standards, once the 5G-AKA is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The UE did not respond to this plain text authentication request, which suggests that it did not accept the insecure communication attempt. This behavior aligns with the 3GPP standards, as the UE should not process unencrypted messages after security mode has been established. The UE's lack of response to the plain text message indicates that it adhered to the security protocols by not engaging in potentially insecure communication. Therefore, based on the 3GPP standards, the UE's action was secure. 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 the test scenario, the interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) involved the UE sending a "security mode complete" message, followed by the AMF sending a "service accept" message. The 5G Authentication and Key Agreement (5G-AKA) process was completed, which is a prerequisite for establishing a secure communication channel. However, the subsequent downlink message from the AMF was sent in plain text, which is unusual given that encryption should be applied after the successful completion of 5G-AKA to ensure confidentiality and integrity of the messages. The UE did not respond to the plain text message, which could indicate a lack of proper handling of unencrypted messages or a failure to maintain the expected security standards. According to the 3GPP standards, once the security context is established, all NAS messages should be encrypted to protect against eavesdropping and tampering. The fact that the UE did not respond to the plain text message could be seen as a security measure, but it also raises concerns about the UE's ability to handle unexpected or non-compliant messages. Overall, the UE's action of not responding to an unencrypted message suggests a potential security issue, as it should have been able to handle such scenarios more robustly. Therefore, based on the 3GPP standards, the UE's communication in this test scenario can be considered "Insecure."
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "registration complete" message, followed by the AMF sending an "identity request" message. Notably, the identity request from the AMF was sent in plain text, and it requested the Subscription Concealed Identifier (SUCI) from the UE. However, the UE did not respond to this request. According to the 3GPP standards, after the completion of the 5G Authentication and Key Agreement (5G-AKA), all NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent an identity request in plain text is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text identity request can be interpreted as a security-conscious action, as responding to such a request could expose sensitive information. By not responding, the UE avoids potential security risks associated with transmitting the SUCI in an unencrypted format. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security as per the 3GPP standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "registration complete" message, followed by the AMF sending an "authentication request" message. Notably, the authentication request was sent in plain text, which is unusual because, according to the 3GPP standards, once the 5G Authentication and Key Agreement (5G-AKA) procedure is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The test indicates that the 5G-AKA was completed, yet the AMF's message was not encrypted, which is a deviation from the expected secure communication protocol. The UE did not respond to the plain-text authentication request, which could be interpreted as a security measure, as responding to an unencrypted message could expose sensitive information. The UE's lack of response suggests that it adhered to the security protocols by not engaging with a potentially insecure communication. Therefore, based on the 3GPP standards, the UE's action of not responding to an unencrypted authentication request aligns with secure communication practices. 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, the UE initially completed the 5G Authentication and Key Agreement (5G-AKA) process, which is a prerequisite for secure communication. Following this, the UE sent a "registration complete" message to the AMF, indicating that it had successfully registered with the network. However, the AMF then sent an "identity request" message to the UE, requesting the Subscription Concealed Identifier (SUCI). Notably, this identity request was sent in plain text, which is unusual because, after the completion of 5G-AKA, messages should be encrypted to ensure confidentiality and integrity. In response to the identity request, the UE sent a "deregistration request (UE originating)" message. This action by the UE suggests that it detected an anomaly or potential security threat, as the identity request was not encrypted, which is against the 3GPP standards for secure communication post-authentication. The UE's decision to deregister rather than provide the requested identity in an unencrypted format indicates a cautious approach to maintaining security. By refusing to transmit sensitive information like the SUCI in plain text, the UE adhered to security protocols designed to protect user identity and data. Therefore, the UE's action in this scenario can be considered secure, as it prioritized the protection of sensitive information over compliance with an insecure request. Secure

179	179	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.265115976333618 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.2653589248657227 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.469132900238037 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a "registration complete" message, indicating the completion of the registration process. Subsequently, the AMF sent a "configuration update command" to the UE. Notably, this downlink message from the AMF was sent as a plain NAS message, without encryption, as indicated by the security header being set to "Plain NAS message (0)." Following this, the UE sent a "deregistration request (UE originating)" back to the AMF. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed, which was noted as completed in the test summary. However, the fact that the AMF sent a plain NAS message suggests that the security context was not properly applied, or there was a deliberate test condition to send it unencrypted. The UE's response with a deregistration request could be interpreted as a security measure, possibly due to the reception of an unencrypted message, which might have been perceived as a security anomaly. Based on the 3GPP standards, the UE should ideally operate within an encrypted context post-5G-AKA completion. The UE's action to deregister could be seen as a cautious response to a potential security issue, aligning with secure behavior. However, the initial acceptance of a plain message without immediate encryption context raises concerns. Overall, the UE's action to deregister suggests an attempt to maintain security, but the acceptance of a plain message indicates a potential vulnerability. Therefore, the communication can be considered "Insecure."
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for secure communication. Following this, the UE sent an uplink NAS transport message, and the AMF responded with a configuration update command. Notably, the configuration update command from the AMF was sent as a plain NAS message, indicated by the security header being set to "Plain NAS message (0)." This means that the message was not encrypted, which is a deviation from the expected secure communication standards outlined by 3GPP, where messages should be encrypted after the completion of 5G-AKA. Subsequently, the UE sent a deregistration request, which was also an uplink NAS transport message. The fact that the AMF sent a plain message suggests a potential vulnerability, as sensitive information could be exposed if intercepted. The UE's action of sending a deregistration request in response to a plain configuration update command could be seen as a security measure to terminate the session, but the initial acceptance of a plain message indicates a lapse in secure communication. Therefore, based on the 3GPP standards, the UE's communication in this scenario can be considered insecure due to the acceptance and processing of an unencrypted message from the AMF. Insecure

181	181	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 3100 RAND: 35353535353535353535353535353535 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 5 UE provided: No response The packet capture during the test using wireshark is: 2.4268798828125 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4271068572998047 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.42726993560791 AMF to UE DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. The UE initially sent an uplink NAS transport message, which was followed by the AMF sending an authentication request. Notably, the authentication request was sent in plain text, which is unusual because, according to the 3GPP standards, messages should be encrypted after the completion of the 5G Authentication and Key Agreement (5G-AKA) process to ensure secure communication. The test summary indicates that the 5G-AKA process was completed, yet the AMF's subsequent message was not encrypted. The UE did not respond to the authentication request, which could suggest that it detected the lack of encryption and chose not to proceed with an insecure communication. This behavior aligns with the security protocols outlined by 3GPP, which emphasize the importance of encrypted communication to protect against potential interception and tampering. Therefore, the UE's decision to not respond to an unencrypted authentication request demonstrates adherence to security standards, indicating that the UE acted securely in this scenario. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several NAS messages. After the 5G Authentication and Key Agreement (5G-AKA) was completed, which is necessary for establishing a secure communication channel, the UE sent an uplink NAS transport message. Subsequently, the AMF responded with a service reject message, which was sent in plain text and included a 5GMM cause code of 111, indicating a protocol error, unspecified. The UE did not provide any response to this service reject message. According to the 3GPP standards, once the 5G-AKA procedure is completed, NAS messages should be encrypted to ensure confidentiality and integrity. However, the AMF's service reject message was sent in plain text, which is a deviation from the expected secure communication protocol. Despite this, the UE's lack of response to the plain text message could be interpreted as a cautious approach, avoiding further communication that might compromise security. However, the initial sending of the uplink NAS transport message without ensuring the encryption status of subsequent messages could be seen as a potential security oversight. Therefore, while the UE's non-response to the plain text message might be considered a secure action, the overall interaction raises concerns about adherence to secure communication practices as per the 5G standard. In conclusion, the UE's actions in this scenario are deemed "Insecure."

183	183	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 0000 RAND: 35353535353535353535353535353535 AUTN: 3030303030303000eeb598a00f560000 ngKSI_TSC: Native security context ngKSI_KSI: 0 UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.5556139945983887 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.555833101272583 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Configuration update command 0.5559549331665039 AMF to UE DownlinkNASTransport, Authentication request 0.7596380710601807 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE sent an uplink NAS transport message, followed by the AMF sending an authentication request. Notably, the authentication request from the AMF was sent in plain text, which is unusual as per the 5G standard outlined by 3GPP, where messages should be encrypted after the 5G Authentication and Key Agreement (5G-AKA) procedure is completed. The 5G-AKA was marked as completed, yet the subsequent authentication request was not encrypted, indicating a potential security lapse. The UE responded with a deregistration request, which could suggest that it detected the anomaly and chose to terminate the session. According to 3GPP standards, once the 5G-AKA is completed, all NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent an unencrypted authentication request after the 5G-AKA completion is a deviation from the standard security protocol. The UE's decision to deregister could be interpreted as a precautionary measure to avoid potential security risks. Therefore, while the UE's action to deregister might be seen as a secure response to an insecure situation, the overall interaction, particularly the unencrypted message from the AMF, indicates a security issue in the communication process. Insecure.

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent an uplink NAS transport message, after which the AMF responded with an identity request message in plain text, requesting the International Mobile Equipment Identity (IMEI) from the UE. Instead of providing the requested identity, the UE responded with a deregistration request, indicating a UE-originated deregistration. This sequence of actions suggests that the UE did not comply with the identity request, which was sent in plain text, potentially due to security concerns. According to the 3GPP standards, NAS messages should be encrypted after the successful completion of the 5G-AKA to ensure confidentiality and integrity. The fact that the AMF sent an identity request in plain text could be perceived as a security risk, and the UE's decision to deregister rather than respond to the request may indicate a protective measure against potential exposure of sensitive information. Therefore, the UE's action can be considered secure as it avoided transmitting sensitive identity information over an unencrypted channel, adhering to the security principles outlined by 3GPP. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS transport message to the AMF. In response, the AMF sent a registration reject message back to the UE, which was transmitted in plain text. The 5GMM Cause code 62 indicates that the rejection was due to "No network slices available." The UE did not provide any response to this rejection. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. However, in this test, the AMF's downlink message was sent in plain text, which is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text message could be interpreted as a failure to maintain secure communication standards, as it did not attempt to re-establish a secure channel or reject the insecure message. Therefore, based on the 3GPP standards, the UE's action in this scenario can be considered insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. After the completion of the 5G Authentication and Key Agreement (5G-AKA), the UE sent an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a security mode command back to the UE. Notably, this downlink message was sent as a plain NAS message, which means it was not encrypted. The UE then responded with a deregistration request, indicating that it did not proceed with the security mode command. According to the 3GPP standards, after the 5G-AKA is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent a plain security mode command suggests a potential vulnerability, as the message was not protected. The UE's decision to deregister rather than proceed with the unprotected security mode command can be seen as a cautious approach to avoid engaging in potentially insecure communication. This behavior aligns with the security principles of the 5G standard, which emphasize the importance of encrypted communication post-authentication. Therefore, the UE's action to deregister in response to receiving an unencrypted security mode command can be considered secure, as it avoided a potentially insecure interaction. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. After the completion of the 5G Authentication and Key Agreement (5G-AKA), which is necessary for establishing a secure communication channel, the UE sent an uplink NAS transport message. Subsequently, the AMF sent an identity request to the UE, requesting the International Mobile Equipment Identity Software Version (IMEISV). Notably, this identity request was sent in plain text, which is a critical point of concern. According to the 3GPP standards, once the 5G-AKA procedure is completed, all NAS messages should be encrypted to ensure confidentiality and integrity. However, the AMF's identity request was not encrypted, potentially exposing sensitive information. The UE, in response, did not provide any response to the identity request. This lack of response from the UE can be interpreted as a security measure, as it avoided transmitting sensitive information over an unencrypted channel. By not responding to the plain text identity request, the UE adhered to the security principles outlined by 3GPP, which emphasize the importance of protecting user identity and equipment information. Therefore, the UE's action of not responding to the unencrypted identity request can be considered secure, as it prevented potential exposure of sensitive information. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. After completing the 5G Authentication and Key Agreement (5G-AKA), which is necessary for establishing a secure communication channel, the UE sent a service request to the AMF. In response, the AMF sent a deregistration accept message back to the UE. Notably, this downlink message from the AMF was sent in plain text, which means it was not encrypted. The UE did not provide any response to this deregistration accept message. According to the 3GPP standards, once the 5G-AKA is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent a plain text message indicates a potential security vulnerability, as it exposes the communication to interception and tampering. The UE's lack of response to the plain text deregistration accept could suggest that it did not recognize or accept the message due to its unencrypted nature, which would be a secure behavior. However, without further information on the UE's internal handling of this situation, it is difficult to definitively conclude the security posture of the UE. Based on the available information, the UE's action of not responding to an unencrypted message aligns with secure communication practices. Therefore, the UE's behavior in this scenario can be considered "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. Subsequently, the AMF responded with a Security Mode Command, which was sent as a plain NAS message. The ciphering and integrity protection algorithms were specified as 5G-EA6 and 128-5G-IA2, respectively. However, the security header indicated that the message was sent in plain text (security header type 0), and the UE did not provide a response to this command. According to the 3GPP standards, after the 5G-AKA procedure, NAS messages should be encrypted and integrity protected to ensure confidentiality and integrity. The fact that the Security Mode Command was sent in plain text and the UE did not respond suggests a potential security vulnerability. The UE's lack of response could indicate a failure to recognize or process the security mode command, which is critical for establishing secure communication. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario appears to be insecure, as it did not adhere to the expected security protocols for encrypted communication following the 5G-AKA process. Insecure

190	190	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication request The downlink message from the AMF was sent as: Plain ABBA: 1010 RAND: 7479eaccb74fb3be01aa8b2b6ff1abcb AUTN: dd84e27507488000bb521f82528f6f6e ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: No response The packet capture during the test using wireshark is: 16.614274978637695 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 16.614504098892212 AMF to UE SACK (Ack=22, Arwnd=106496) , DownlinkNASTransport, Authentication request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the test scenario, the User Equipment (UE) initiated a service request to the Access and Mobility Management Function (AMF) after completing the 5G Authentication and Key Agreement (5G-AKA) process. The AMF responded with an authentication request message, which was sent in plain text. The UE, however, did not provide any response to this authentication request. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent the authentication request in plain text indicates a deviation from the expected secure communication protocol. The UE's lack of response to the plain text authentication request suggests that it correctly identified the security anomaly and refrained from engaging in potentially insecure communication. This behavior aligns with the security principles outlined by 3GPP, which emphasize the importance of encrypted communication post-authentication. Therefore, the UE's action of not responding to an unencrypted message can be considered secure, as it prevents potential exposure of sensitive information. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request. Following this, the AMF responded with an authentication request, which was sent in plain text. The authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI values. The UE then responded with an authentication failure message, indicating that the ngKSI was already in use. This response suggests that the UE detected a potential issue with the security context, as the ngKSI (NAS key set identifier) is used to identify the security context for NAS signaling. The fact that the UE flagged the ngKSI as already in use implies that it recognized a potential replay attack or a misconfiguration, where the same security context was being reused improperly. According to the 3GPP standards, the UE should ensure that each authentication request is unique and that the security context is not reused inappropriately. By rejecting the authentication request due to the ngKSI being already in use, the UE adhered to the security protocols designed to prevent replay attacks and ensure the integrity of the authentication process. Therefore, the action taken by the UE was in line with the 3GPP standards for secure communication. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF issuing an identity request. The identity request from the AMF was sent in plain text, requesting the Temporary Mobile Subscriber Identity (TMSI) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, after the completion of the 5G Authentication and Key Agreement (5G-AKA), all Non-Access Stratum (NAS) messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent the identity request in plain text suggests a potential vulnerability, as sensitive information like the TMSI should be protected. The UE's lack of response to the plain text identity request can be interpreted as a security measure to avoid exposing sensitive information over an unencrypted channel. This behavior aligns with the security principles outlined by 3GPP, which emphasize the protection of subscriber identity and data. Therefore, the UE's action of not responding to the plain text identity request can be considered a secure response to an insecure request from the AMF. Secure

193	193	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 9.49011492729187 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.490720987319946 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with a configuration update command. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to this exchange, which is a prerequisite for ensuring that subsequent NAS messages are encrypted and integrity protected. The packet capture indicates that the AMF's downlink message was sent as "Protected," but the security header was marked as "Unknown," and the UE did not provide a response. According to the 3GPP standards, after the successful completion of 5G-AKA, the UE should be able to process protected messages, which include encryption and integrity protection. The lack of response from the UE suggests that it may not have been able to process the protected message correctly, possibly due to an issue with the security header or the encryption keys. This behavior could indicate a potential security vulnerability, as the UE should be capable of handling such messages securely. Therefore, based on the interaction and the UE's lack of response, it appears that the UE's actions were insecure according to the 5G standard. Insecure
194	194	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 18.81248188018799 UE to AMF UplinkNASTransport, Service request 18.8126699924469 AMF to UE SACK (Ack=18, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with an authentication reject message. The 5G-AKA procedure, which is essential for establishing a secure communication channel, was completed prior to this exchange. However, the authentication reject message from the AMF was sent in plain text, which is unusual given that messages should be encrypted after the successful completion of 5G-AKA. The UE did not respond to the authentication reject message, which could be interpreted as a lack of action or a failure to process the message. According to the 3GPP standards, after the 5G-AKA procedure, the UE should expect encrypted messages, and any plain text message could be considered suspicious or indicative of a security breach. The UE's lack of response to the plain text authentication reject message suggests that it did not proceed with any further actions that could compromise security, such as sending sensitive information over an unencrypted channel. Therefore, the UE's behavior aligns with maintaining security by not engaging further with potentially insecure communication. Based on this analysis, the UE's action was "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated communication by sending a service request to the AMF. In response, the AMF sent an identity request to the UE, requesting the Subscription Concealed Identifier (SUCI). Notably, this identity request was sent in plain text, which is a critical point of analysis. The UE then responded with an identity response. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages, including identity requests and responses, should be encrypted to ensure confidentiality and integrity. However, in this test, the identity request from the AMF was sent in plain text, which could potentially expose sensitive information if intercepted. The UE's action of responding to a plain text identity request could be considered insecure, as it did not ensure that the communication was encrypted, thereby potentially compromising the confidentiality of the SUCI. Therefore, based on the 3GPP standards and the observed interaction, the UE's action was insecure. Insecure
196	196	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 9.49011492729187 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 9.490720987319946 AMF to UE SACK (Ack=17, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with a configuration update command. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is a prerequisite for ensuring that subsequent NAS (Non-Access Stratum) messages are encrypted and integrity protected. The packet capture indicates that the AMF's downlink message was sent as "Protected," but the security header was marked as "Unknown," and the UE did not provide a response. According to the 3GPP standards, after the successful completion of 5G-AKA, the UE should be able to decrypt and respond to protected messages from the AMF. The lack of response from the UE suggests that it either failed to decrypt the message or did not recognize the security header, which could indicate a potential issue with the UE's handling of security procedures. This behavior is not aligned with the expected secure communication standards outlined by 3GPP, as the UE should have been able to process and respond to the protected message. Therefore, based on the observed interaction, the UE's action appears to be insecure. Insecure

197	197	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0005860328674316406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Unknown) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. This is a standard procedure where the UE attempts to register with the network. However, the AMF, which was under test control, responded with a deregistration request. Notably, this downlink message from the AMF was protected, as indicated by the security header being both integrity protected and ciphered. Despite this, the 5G Authentication and Key Agreement (5G-AKA) process had not been completed, which is crucial for establishing a secure communication channel. The UE did not respond to the deregistration request, which could be interpreted as a lack of action or a deliberate choice to not engage further without a completed 5G-AKA. According to the 3GPP standards, the 5G-AKA process is essential for ensuring that messages are encrypted and integrity protected, thereby securing the communication. Since the 5G-AKA was not completed, the UE's decision to not respond to the deregistration request can be seen as a cautious approach to avoid engaging in potentially insecure communication. Therefore, based on the 3GPP standards, the UE's lack of response in this scenario aligns with maintaining security protocols, as it avoided further communication without proper authentication and encryption in place. Secure
198	198	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.15979790687561035 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.16023778915405273 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. After the completion of the 5G Authentication and Key Agreement (5G-AKA), which is necessary for establishing a secure communication channel, the UE sent a "security mode complete" message to the AMF. This indicates that the UE accepted the security parameters proposed by the AMF. Subsequently, the AMF sent an "identity request" message to the UE, requesting the Globally Unique Temporary Identifier (GUTI) from the UE. Notably, this identity request was sent in plain text, which is a critical point of concern. According to the 3GPP standards, once the security mode is complete, all subsequent NAS messages should be encrypted to protect the integrity and confidentiality of the communication. The UE, however, did not respond to the identity request, which could be interpreted as a security measure to avoid sending sensitive information over an unencrypted channel. This lack of response suggests that the UE adhered to the security protocols by not transmitting potentially sensitive information in an insecure manner. Therefore, based on the 3GPP standards and the actions taken by the UE, the UE's behavior can be considered secure, as it avoided compromising its identity information over an unprotected channel. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After the successful completion of the 5G Authentication and Key Agreement (5G-AKA), the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters and was ready for secure communication. However, the subsequent message from the AMF was an "identity request" sent in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. The UE did not respond to this request. According to the 3GPP standards, once the security mode is complete, all subsequent NAS messages should be encrypted to protect the integrity and confidentiality of the communication. The fact that the AMF sent an identity request in plain text after the security mode was completed is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text identity request can be interpreted as a security measure to avoid exposing sensitive information in an unencrypted format. This behavior aligns with the 3GPP standards, which emphasize the importance of maintaining secure communication post-authentication. Therefore, the UE's action of not responding to an unencrypted identity request is considered secure. Secure
200	200	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.1511218547821045 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15138006210327148 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After completing the 5G Authentication and Key Agreement (5G-AKA), the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with secure communication. However, the subsequent message from the AMF was an "identity request" sent in plain text, requesting the Subscription Concealed Identifier (SUCI) from the UE. The UE did not respond to this request. According to the 3GPP standards, once the 5G-AKA is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The AMF's decision to send an identity request in plain text is a deviation from this standard, potentially exposing sensitive information. The UE's lack of response to the plain text identity request can be interpreted as a security measure to avoid transmitting sensitive information without encryption. This behavior aligns with the 3GPP security standards, as the UE refrained from responding to an insecure request. Therefore, the UE's action in this scenario was secure. Secure

201	201	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 0.15867114067077637 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15893101692199707 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. After the completion of the 5G Authentication and Key Agreement (5G-AKA), which is necessary for establishing a secure communication channel, the UE sent a "security mode complete" message to the AMF. This indicates that the UE was ready to proceed with secure communication. However, the subsequent message from the AMF was an "identity request" sent in plain text, requesting the International Mobile Equipment Identity (IMEI) from the UE. The UE did not respond to this request. According to the 3GPP standards, once the 5G-AKA is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent an identity request in plain text is a deviation from this standard, potentially exposing sensitive information. The UE's lack of response to the plain text identity request can be interpreted as a security-conscious action, as responding could have compromised its IMEI. By not responding, the UE avoided transmitting sensitive information over an unencrypted channel, aligning with the security principles outlined by 3GPP. Therefore, the UE's action in this scenario was secure. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with secure communication. However, the subsequent message from the AMF was an "identity request" sent in plain text, requesting the Subscription Concealed Identifier (SUCI) from the UE. The UE did not respond to this request. According to the 3GPP standards, once the 5G-AKA process is completed, all subsequent NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The AMF's request for the SUCI in plain text is a deviation from this standard, as it exposes sensitive information to potential interception. The UE's lack of response to the plain text identity request can be interpreted as a security measure to prevent the exposure of sensitive information. By not responding, the UE avoids transmitting the SUCI in an unprotected manner, adhering to the security principles outlined by 3GPP. Therefore, the UE's action in this scenario can be considered secure, as it maintained the confidentiality of the SUCI by not responding to an insecure request. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "security mode complete" message, indicating that it had accepted the security parameters set by the network. Subsequently, the AMF sent an "identity request" message to the UE, requesting the Globally Unique Temporary Identifier (GUTI) from the UE. Notably, this identity request was sent in plain text, which is a critical point of concern. According to the 3GPP standards, once the 5G-AKA process is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The UE, however, did not respond to the identity request, which could be interpreted as a security measure to avoid sending sensitive information over an unencrypted channel. This lack of response from the UE suggests that it adhered to the security protocols by not transmitting its identity in an insecure manner. Therefore, based on the 3GPP standards and the actions taken by the UE, the UE's behavior can be considered secure as it avoided potential exposure of sensitive information. Secure
204	204	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.15074801445007324 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.15094995498657227 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "security mode complete" message to the AMF, indicating that it had successfully established a secure communication channel. However, the subsequent message from the AMF was an "identity request" sent in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. The UE did not respond to this request. According to the 3GPP standards, once the 5G-AKA process is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The AMF's decision to send an identity request in plain text is a deviation from this standard, potentially exposing sensitive information. The UE's lack of response to the plain text identity request can be interpreted as a security measure to prevent the exposure of its IMEISV in an unencrypted format. This behavior aligns with the 3GPP security standards, as the UE refrained from transmitting sensitive information over an insecure channel. Therefore, the UE's action in this scenario was secure. Secure

205	205	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4575481414794922 UE to AMF UplinkNASTransport, Registration complete 0.4577751159667969 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "registration complete" message, followed by the AMF sending an "identity request" message. Notably, the identity request from the AMF was sent in plain text, and it requested the Subscription Concealed Identifier (SUCI) from the UE. However, the UE did not respond to this request. According to the 3GPP standards, after the 5G Authentication and Key Agreement (5G-AKA) procedure is completed, subsequent NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent the identity request in plain text is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text identity request can be interpreted as a security-conscious action, as responding to such a request could expose sensitive information like the SUCI. By not responding, the UE avoids potential security vulnerabilities that could arise from transmitting sensitive data in an unencrypted format. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security as per the 3GPP standards. Secure
206	206	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4691789150238037 UE to AMF UplinkNASTransport, Registration complete 0.46941208839416504 AMF to UE SACK (Ack=5, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "registration complete" message, followed by the AMF sending an "identity request" message. Notably, the identity request from the AMF was sent in plain text, which is a critical point of analysis. According to the 3GPP standards, once the 5G Authentication and Key Agreement (5G-AKA) procedure is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The AMF's request for the Subscription Concealed Identifier (SUCI) in plain text is a deviation from the expected secure communication protocol. The UE's lack of response to this plain text identity request can be interpreted as a security-conscious action, as responding to an unencrypted identity request could expose sensitive information. By not responding, the UE avoids potential exposure of the SUCI, which aligns with the security principles of protecting user identity and data. Therefore, the UE's decision to withhold a response to an unencrypted identity request is consistent with maintaining security as per the 3GPP standards. Secure

207	207	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 2.019134998321533 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.0193519592285156 AMF to UE SACK (Ack=7, Arwnd=106361) , DownlinkNASTransport, Identity request 3.000807046890259 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test of a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "registration complete" message to the AMF, which then responded with an "identity request" message. Notably, this identity request was sent in plain text, which is a critical point of concern. The AMF requested the Subscription Concealed Identifier (SUCI) from the UE, but the UE did not provide a response. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent an identity request in plain text suggests a potential vulnerability, as sensitive information like the SUCI should not be exposed in an unencrypted format. The UE's lack of response to the plain text identity request can be interpreted as a security measure, as responding to such a request could compromise the UE's identity privacy. Therefore, the UE's decision to withhold a response aligns with the security principles outlined by 3GPP, as it avoids transmitting sensitive information over an unprotected channel. Based on this analysis, the UE's action was secure. Secure
208	208	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.4989509582519531 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.49918699264526367 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "registration complete" message to the AMF, which is a standard procedure indicating that the UE has successfully registered with the network. Subsequently, the AMF sent an "identity request" message to the UE, requesting the Subscription Concealed Identifier (SUCI). Notably, this identity request was sent in plain text, which is unusual because, according to 3GPP standards, once the 5G-AKA process is completed, all NAS messages should be encrypted to ensure confidentiality and integrity. The UE did not respond to this identity request, which could be interpreted as a security measure to avoid transmitting sensitive information over an unencrypted channel. This behavior aligns with the 3GPP security standards, which emphasize the importance of protecting subscriber identity and other sensitive information. By not responding to an unencrypted identity request, the UE demonstrated adherence to these security principles, thereby maintaining the confidentiality of the subscriber's identity. Therefore, the action taken by the UE was secure. Secure

209	209	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.48286890983581543 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.48304104804992676 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "registration complete" message to the AMF, which was followed by an "identity request" from the AMF. Notably, the identity request was sent in plain text, and the AMF requested the Subscription Concealed Identifier (SUCI) from the UE. However, the UE did not respond to this request. According to the 3GPP standards, after the 5G-AKA process is completed, NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent an identity request in plain text is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text identity request can be interpreted as a security measure, as responding to such a request could expose sensitive information. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security as per the 3GPP standards, which emphasize the importance of encrypted communication post-authentication. Secure
210	210	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.48984408378601074 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.4900491237640381 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent a "registration complete" message to the AMF, which was followed by an "identity request" from the AMF. Notably, the identity request was sent in plain text, and the AMF requested the Subscription Concealed Identifier (SUCI) from the UE. However, the UE did not respond to this request. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent an identity request in plain text is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text identity request can be interpreted as a security measure, as responding to such a request could expose sensitive information. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security as per the 3GPP standards. In this context, the UE's behavior can be considered secure. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. After the 5G Authentication and Key Agreement (5G-AKA) was completed, the UE sent a "registration complete" message to the AMF. Subsequently, the AMF sent an "identity request" message to the UE, requesting the Temporary Mobile Subscriber Identity (TMSI). Notably, this identity request was sent in plain text, which is a critical point of concern. According to the 3GPP standards, once the 5G-AKA procedure is completed, all NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. However, the AMF's identity request was not encrypted, which could expose sensitive information if intercepted. The UE did not respond to this plain text identity request, which can be interpreted as a security-conscious action, as responding to an unencrypted request could compromise the UE's identity. By not responding, the UE avoided potential exposure of its TMSI in an insecure manner. Therefore, based on the 3GPP standards and the actions taken by the UE, the UE's decision to withhold a response to an unencrypted identity request aligns with secure communication practices. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a downlink NAS transport message, an identity request, which was transmitted in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. Notably, the UE did not provide a response to this request. According to the 3GPP standards, once the 5G-AKA process is completed, NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent the identity request in plain text could be considered a security vulnerability, as it exposes sensitive information to potential interception. However, the UE's lack of response to the plain text identity request can be interpreted as a security-conscious action, as it avoids transmitting sensitive information without encryption. This behavior aligns with the security principles outlined by 3GPP, which emphasize the protection of user identity and equipment information. Therefore, the UE's decision not to respond to an unencrypted identity request demonstrates adherence to secure communication practices. Secure.

213	213	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: SUCI UE provided: No response The packet capture during the test using wireshark is: 0.7595288753509521 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.7598080635070801 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. Subsequently, the AMF responded with an identity request message, which was sent in plain text, requesting the Subscription Concealed Identifier (SUCI) from the UE. However, the UE did not provide any response to this request. According to the 3GPP standards, once the 5G-AKA process is completed, NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent the identity request in plain text is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text identity request can be interpreted as a security measure, as responding to an unencrypted request could expose sensitive information. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security as per the 3GPP standards. Secure
214	214	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.7997701168060303 UE to AMF UplinkNASTransport, UL NAS transport, PDU session establishment request 0.8000459671020508 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE initiated an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a downlink NAS transport message, an identity request, which was transmitted in plain text, requesting the Temporary Mobile Subscriber Identity (TMSI) from the UE. However, the UE did not provide any response to this identity request. According to the 3GPP standards, once the 5G-AKA process is completed, NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent the identity request in plain text could be considered a security vulnerability, as it exposes sensitive information to potential interception. However, the UE's lack of response to the plain text identity request can be interpreted as a security measure, as it avoids transmitting potentially sensitive information without encryption. This behavior aligns with the security principles of the 5G standard, which emphasize the protection of subscriber identity and data. Therefore, the UE's action of not responding to an unencrypted identity request can be considered secure according to the 3GPP standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent an uplink NAS transport message, which was followed by the AMF sending an identity request to the UE. Notably, the identity request from the AMF was sent in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, after the 5G-AKA process is completed, NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent the identity request in plain text could potentially expose sensitive information if the UE were to respond. The UE's lack of response to the plain text identity request can be interpreted as a security measure to prevent the exposure of its IMEISV in an unencrypted format. This behavior aligns with the security principles outlined by 3GPP, which emphasize the protection of user identity and equipment information. Therefore, the UE's action of not responding to the plain text identity request can be considered secure, as it avoids the risk of transmitting sensitive information without encryption. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent an uplink NAS transport message, which was followed by the AMF sending an identity request message to the UE. Notably, the identity request from the AMF was sent in plain text, requesting the Subscription Concealed Identifier (SUCI) from the UE. However, the UE did not respond to this request. According to the 3GPP standards, after the 5G-AKA process is completed, NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent an identity request in plain text is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text identity request can be interpreted as a security measure to avoid exposing sensitive information like the SUCI in an unencrypted format. This behavior aligns with the security principles outlined by 3GPP, which emphasize the protection of subscriber identity and data. Therefore, the UE's action of not responding to an unencrypted identity request is considered secure, as it prevents potential exposure of sensitive information. Secure

217	217	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.531268835067749 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5314879417419434 AMF to UE SACK (Ack=6, Arwnd=106361) , DownlinkNASTransport, Configuration update command 0.5316059589385986 AMF to UE DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test of a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent an uplink NAS transport message, which was followed by the AMF sending an identity request message to the UE. Notably, the identity request from the AMF was sent in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not respond to this request. According to the 3GPP standards, after the 5G-AKA process is completed, NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent an identity request in plain text could be considered a security vulnerability, as it exposes sensitive information to potential interception. The UE's lack of response to the plain text identity request can be interpreted as a security-conscious action, as it avoids transmitting sensitive information without encryption. This behavior aligns with the security principles outlined by 3GPP, which emphasize the protection of user identity and equipment information. Therefore, the UE's decision not to respond to an unencrypted identity request demonstrates adherence to secure communication practices. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. After the 5G Authentication and Key Agreement (5G-AKA) was completed, which is necessary for securing NAS messages, the UE sent an uplink NAS transport message. Subsequently, the AMF sent an identity request to the UE, requesting the Temporary Mobile Subscriber Identity (TMSI). Notably, this identity request was sent in plain text, which is unusual given that the 5G-AKA was completed, and messages should typically be encrypted to ensure confidentiality and integrity. The UE, however, did not respond to this identity request. According to the 3GPP standards, once the 5G-AKA is completed, NAS messages should be encrypted to protect sensitive information such as the TMSI. The UE's lack of response to an unencrypted identity request can be seen as a security-conscious action, as responding to a plain text request could expose sensitive information. Therefore, the UE's decision not to respond to the unencrypted identity request aligns with maintaining security standards by not transmitting potentially sensitive information over an insecure channel. Based on this analysis, the UE's action was "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The UE sent an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. In response, the AMF sent a downlink NAS transport message, an identity request, which was transmitted in plain text, requesting the Temporary Mobile Subscriber Identity (TMSI) from the UE. However, the UE did not provide any response to this identity request. According to the 3GPP standards, once the 5G-AKA process is completed, NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent the identity request in plain text could be considered a security vulnerability, as it exposes sensitive information to potential interception. However, the UE's lack of response to the plain text identity request can be interpreted as a security measure, as it avoids transmitting potentially sensitive information without encryption. This behavior aligns with the security principles of the 5G standard, which emphasize the protection of subscriber identity and data. Therefore, the UE's action of not responding to an unencrypted identity request can be considered secure. Secure
220	220	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.6309528350830078 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.63124680519104 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. After the 5G Authentication and Key Agreement (5G-AKA) was completed, the UE sent an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. Subsequently, the AMF responded with a downlink NAS transport message, an identity request, which was sent in plain text. The AMF requested the Temporary Mobile Subscriber Identity (TMSI) from the UE, but the UE did not provide a response. According to the 3GPP standards, once the 5G-AKA procedure is completed, NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent the identity request in plain text could be a deliberate part of the test to assess the UE's response to an insecure request. The UE's lack of response to the identity request can be interpreted as a security measure, as responding to an unencrypted identity request could expose sensitive information. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security as per the 3GPP standards, which emphasize the importance of encrypted communication post-authentication. 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 the described security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with a service accept message. The test indicates that the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is a prerequisite for establishing a secure communication channel. However, the packet capture reveals that the downlink message from the AMF, specifically the service accept message, was sent in plain text rather than being encrypted. According to the 3GPP standards, once the 5G-AKA procedure is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The UE's lack of response to the plain text message suggests that it did not reject or flag the unencrypted message, which could imply a security vulnerability. The UE should ideally expect encrypted messages post-authentication and take appropriate action if this is not the case. Therefore, based on the 3GPP standards and the observed behavior, the UE's action in this scenario appears to be insecure, as it did not enforce the expected security measures after the 5G-AKA completion. Insecure
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 the described security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with a service accept message. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to this exchange, which is a prerequisite for ensuring that subsequent NAS (Non-Access Stratum) messages are encrypted. However, the service accept message from the AMF was sent in plain text, and the UE did not provide any response to this message. According to the 3GPP standards, once the 5G-AKA procedure is completed, NAS messages should be encrypted to maintain confidentiality and integrity. The fact that the AMF sent a plain text message and the UE did not respond suggests a potential security issue. The UE's lack of response could indicate that it detected the plain text message as a security anomaly and chose not to proceed, which would be a secure behavior. However, without further information on the UE's internal decision-making process, it is difficult to definitively conclude whether the UE's action was secure. Based on the available information, the UE's lack of response to an unencrypted message aligns with secure behavior as per 3GPP standards, which prioritize encrypted communication post-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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF responded with a service reject message, indicating that the UE identity could not be derived by the network. Notably, this downlink message from the AMF was sent in plain text, which is unusual given that the 5G-AKA process was completed, suggesting that encryption should have been in place for subsequent NAS messages. The 5GMM Cause code 9, which corresponds to "UE identity cannot be derived by the network," further supports the notion that there was an issue with the UE's identity recognition. The UE did not provide any response to the service reject message. According to the 3GPP standards, once the 5G-AKA process is completed, NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF's message was sent in plain text raises concerns about the security of the communication. However, since the UE did not respond to the plain text message, it suggests that the UE may have recognized the security anomaly and chose not to engage further, which aligns with secure behavior. Therefore, based on the UE's lack of response to an unencrypted message, the UE's action can be considered secure. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF responded with a service reject message, indicating that the UE identity could not be derived by the network, with a 5GMM Cause value of 9. Notably, the downlink message from the AMF was sent in plain text, which is a critical point of analysis. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. However, in this test, the AMF's service reject message was sent unencrypted, which could expose sensitive information to potential eavesdroppers. The UE did not provide any response to the service reject message, which might be a standard behavior when the UE identity cannot be derived, but it also means the UE did not attempt to re-establish a secure connection or address the lack of encryption. Given that the UE did not take any action to ensure the security of the communication after receiving an unencrypted message, the UE's behavior can be considered insecure according to the 3GPP standards, which emphasize the importance of encryption in NAS communications post-authentication. Therefore, the UE's action in this scenario is deemed "Insecure."

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF responded with a service reject message, which was sent in plain text, indicating a protocol error with an unspecified cause (5GMM Cause: 111). The UE did not provide any response to this service reject message. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. However, in this test, the downlink message from the AMF was sent in plain text, which is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text service reject message could be interpreted as a failure to recognize or handle the security breach appropriately. This suggests that the UE did not adhere to the security standards outlined by 3GPP, as it should have either rejected the unencrypted message or taken corrective action to ensure secure communication. Therefore, based on the interaction and the UE's response, the action taken by the UE was insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with a service reject message. The 5G Authentication and Key Agreement (5G-AKA) process was completed prior to this exchange, which is a prerequisite for ensuring that subsequent NAS messages are encrypted. However, the service reject message from the AMF was sent in plain text, indicating that it was not encrypted. The 5GMM Cause code 21, which typically indicates a synchronization failure, was provided by the AMF. The UE did not respond to the service reject message. According to the 3GPP standards, once the 5G-AKA is completed, NAS messages should be encrypted to maintain confidentiality and integrity. The fact that the service reject message was sent in plain text suggests a potential security vulnerability, as it exposes the communication to interception and tampering. The UE's lack of response to the plain text message could be interpreted as a failure to recognize or handle the security breach appropriately. Therefore, based on the 3GPP standards, the UE's action in this scenario appears to be insecure, as it did not ensure the confidentiality and integrity of the communication. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. The test began with the completion of the 5G Authentication and Key Agreement (5G-AKA), which is a prerequisite for secure communication. Following this, the UE sent an uplink NAS transport message to the AMF. In response, the AMF sent a security mode command to the UE, which was protected, indicating that encryption was applied. The security mode command is crucial as it establishes the security algorithms to be used for subsequent communications. The AMF specified the use of the 5G-EA6 ciphering algorithm and the 128-5G-IA2 integrity algorithm. However, the UE did not provide a response to the security mode command, which is a critical step in the security procedure. According to the 3GPP standards, the UE should respond to the security mode command to confirm the security algorithms and proceed with secure communication. The absence of a response from the UE suggests a failure to complete the security handshake, leaving the communication potentially vulnerable. Therefore, based on the 3GPP standards, the action taken by the UE was insecure as it did not adhere to the required security protocol by failing to respond to the security mode command. Insecure

228	228	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 00f2 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 5G- IA0 (null) Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 2.722198963165283 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.7225029468536377 AMF to UE SACK (Ack=8, Arwnd=106361) , DownlinkNASTransport, Configuration update command 2.722743034362793 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS transport message, which was acknowledged by the AMF. Subsequently, the AMF sent a security mode command to the UE, which is intended to establish security algorithms for encryption and integrity protection of NAS messages. However, the security mode command was sent as a protected message, but the cipher and integrity algorithms used were 5G-EA0 and 5G-IA0, respectively, both of which are null algorithms. This means that no actual encryption or integrity protection was applied to the messages. Additionally, the UE did not provide a response to the security mode command, which is a critical step in confirming the establishment of secure communication. According to the 3GPP standards, the use of null algorithms and the lack of a response from the UE indicate a failure to establish a secure communication channel. Therefore, based on the interaction and the standards outlined by 3GPP, the action taken by the UE was insecure. Insecure
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 the test scenario, the interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) involved the UE sending a service request to the AMF, followed by the AMF responding with a configuration update command. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to these exchanges, which is a prerequisite for establishing a secure communication channel. However, the configuration update command from the AMF was sent as a plain NAS message, indicated by the security header being set to "Plain NAS message (0)." This means that the message was not encrypted, despite the 5G-AKA procedure having been completed, which should have enabled encryption for subsequent NAS messages. The UE did not provide any response to the plain configuration update command. According to the 3GPP standards, once the 5G-AKA procedure is completed, NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the UE did not respond to an unencrypted message could be interpreted as a security measure, as it did not engage with a potentially insecure communication. However, the lack of encryption in the AMF's message itself is a security concern. Given that the UE did not respond to the plain message, it suggests that the UE maintained a secure posture by not acknowledging or acting upon an unencrypted command. Therefore, based on the UE's action of not responding to the plain message, the UE's behavior can be considered secure according to the 3GPP standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS message indicating "registration complete" to the AMF. Subsequently, the AMF responded with a downlink NAS message, specifically a "security mode command," which was sent in plain text. The security mode command is intended to establish encryption and integrity protection for subsequent NAS messages. However, the UE did not respond to this command. According to the 3GPP standards, after the 5G-AKA process, all NAS messages should be encrypted and integrity protected to ensure confidentiality and authenticity. The fact that the AMF sent the security mode command in plain text and the UE did not respond suggests a potential security lapse. The UE's lack of response could indicate a failure to recognize or process the security mode command, which is critical for securing further communication. Therefore, based on the 3GPP standards, the UE's action in this scenario appears to be insecure, as it did not proceed with the necessary steps to establish a secure communication channel after the initial authentication. Insecure

231	231	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 3100 Cipher Algorithm: 5G-EA6 Integrity Algorithm: 5G-IA5 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.4284870624542236 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4289300441741943 AMF to UE SACK (Ack=11, Arwnd=106401) , DownlinkNASTransport, Configuration update command 2.4293291568756104 AMF to UE DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS transport message to the AMF. Subsequently, the AMF responded with a security mode command, which was sent as a plain NAS message. The security mode command is intended to establish encryption and integrity protection for subsequent NAS messages. However, the UE did not respond to this command. According to the 3GPP standards, after the 5G-AKA process, all NAS messages should be encrypted and integrity protected to ensure confidentiality and integrity. The fact that the security mode command was sent in plain text and the UE did not respond indicates a potential security lapse. The UE's lack of response to the security mode command suggests that it did not proceed to establish the necessary security context, leaving the communication vulnerable. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario was 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. Subsequently, the AMF responded with an authentication reject message, which was sent in plain text. The UE did not provide any response to this message. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. However, in this test, the AMF sent the authentication reject message in plain text, which is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text message could be interpreted as a security measure, as it did not engage further in potentially insecure communication. This behavior aligns with the 3GPP standards, which emphasize the importance of secure communication. Therefore, the UE's action of not responding to an unencrypted message can be considered secure, as it avoided engaging in a potentially insecure exchange. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. Subsequently, the AMF responded with an authentication reject message, which was sent in plain text. The UE did not provide any response to this message. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. However, in this test, the AMF sent the authentication reject message in plain text, which is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text message can be interpreted as a secure action, as it did not engage further in potentially insecure communication. By not responding, the UE avoided any further exchange of information that could be intercepted or manipulated. Therefore, based on the 3GPP standards and the UE's behavior in this scenario, the UE's action can be considered secure, as it adhered to the principle of not engaging in unencrypted communication after the 5G-AKA process. Secure
234	234	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.1599588394165039 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.160261869430542 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response, followed by the AMF sending an identity request. The identity request from the AMF was sent in plain text, and it requested the Temporary Mobile Subscriber Identity (TMSI) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed before any NAS messages can be encrypted. Since the 5G-AKA was not completed, the messages were not encrypted, which is why the identity request was sent in plain text. The UE's lack of response to the identity request could be interpreted as a security measure, as responding to an unencrypted identity request could expose sensitive information. By not responding, the UE potentially avoided disclosing its TMSI in an insecure manner. Therefore, based on the 3GPP standards and the context of the test, the UE's action of not responding to the plain text identity request can be considered a secure behavior, as it prevented the exposure of sensitive information before the completion of the 5G-AKA process. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response, followed by the AMF sending an identity request. The identity request from the AMF was sent in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to ensure that subsequent NAS messages are encrypted. Since the 5G-AKA was not completed, the identity request was sent in plain text, which is a potential security risk as it could expose sensitive information if intercepted. The UE's lack of response to the identity request can be seen as a security-conscious action, as it avoided transmitting potentially sensitive information over an unencrypted channel. This behavior aligns with the security principles of minimizing exposure of sensitive data when encryption is not in place. Therefore, the UE's action of not responding to the identity request in this context can be considered secure, as it prevented the transmission of sensitive information in an insecure manner. Secure
236	236	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0173 Cipher Algorithm: 5G-EA4 Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.15990495681762695 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1602330207824707 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command 0.3627040386199951 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is crucial for establishing a secure communication channel. Following this, 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 NAS message, indicating that it was not encrypted. The UE subsequently sent a deregistration request, which was also an uplink NAS transport message. According to the 3GPP standards, after the 5G-AKA process, all NAS messages should be encrypted to ensure confidentiality and integrity. However, the security mode command from the AMF was sent in plain text, which is a deviation from the expected secure communication protocol. This lack of encryption in the downlink message could potentially expose sensitive information to interception or manipulation. Therefore, despite the UE's adherence to the protocol by completing the 5G-AKA, the overall communication was insecure due to the AMF's failure to encrypt the security mode command. Insecure

237	237	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0000 Cipher Algorithm: 5G-EA5 Integrity Algorithm: 5G- IA0 (null) Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.12820696830749512 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12850189208984375 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. Subsequently, the AMF sent a security mode command to the UE, which was protected, indicating that encryption was applied to the message. The security mode command is a critical step where the AMF instructs the UE to apply specific security algorithms for ciphering and integrity protection. In this test, the ciphering algorithm used was 5G-EA5, while the integrity algorithm was 5G-IA0, which is a null algorithm, meaning no integrity protection was applied. The UE, however, did not provide a response to the security mode command. According to the 3GPP standards, the UE should respond to the security mode command to establish a secure communication channel. The lack of response from the UE suggests a failure to comply with the expected security procedures, potentially leaving the communication unprotected. The use of a null integrity algorithm further exacerbates the situation, as it does not provide any integrity protection, which is crucial for ensuring the authenticity and integrity of the messages. Therefore, based on the 3GPP standards, the UE's actions in this scenario were insecure, as it failed to establish a secure communication channel by not responding to the security mode command and relying on a null integrity algorithm. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at the time of this interaction, which is crucial for establishing a secure communication channel. The AMF's identity request was sent in plain text, requesting the Temporary Mobile Subscriber Identity (TMSI) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, the 5G-AKA procedure must be completed to ensure that messages are encrypted, thereby protecting sensitive information such as the TMSI. The UE's lack of response to the plain text identity request can be interpreted as a security measure, as responding with sensitive information over an unencrypted channel would be insecure. By not responding, the UE avoids exposing its TMSI in an unprotected manner, aligning with the security principles outlined by 3GPP. Therefore, the UE's action in this scenario can be considered secure, as it refrains from transmitting sensitive information without the assurance of encryption. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. The AMF's identity request was sent in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed first. Since the 5G-AKA was not completed, the communication was not encrypted, and the AMF's request was sent in plain text. The UE's lack of response to the identity request can be seen as a security measure, as responding to an unencrypted request could expose sensitive information. By not responding, the UE avoids the risk of transmitting its IMEISV in an insecure manner. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security standards by not exposing sensitive information without encryption. Secure
240	240	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0363 Cipher Algorithm: 128-5G-EA3 Integrity Algorithm: 128-5G-IA1 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.12767410278320312 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1279001235961914 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. Subsequently, the AMF sent a security mode command to the UE. Notably, the security mode command was sent as a plain NAS message, indicated by the security header being set to "Plain NAS message (0)." The UE, however, did not provide any response to this command. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The use of a plain NAS message for the security mode command suggests a potential vulnerability, as it exposes the message to interception and tampering. The UE's lack of response could be interpreted as a failure to engage in secure communication, as it did not proceed with the expected encrypted communication following the security mode command. This behavior indicates a deviation from the secure communication practices outlined by the 3GPP standards, which require encryption post-authentication. Therefore, based on the interaction and the standards, the action taken by the UE 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was focused on the NAS (Non-Access Stratum) security procedures. Initially, the 5G Authentication and Key Agreement (5G-AKA) was completed, which is a prerequisite for secure communication. The UE then sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters previously provided by the AMF. However, the AMF subsequently sent a "security mode command" back to the UE, which was protected, meaning it was encrypted and integrity protected. The UE, however, did not respond to this command. The use of the cipher algorithm 5G-EA7 and integrity algorithm 128-5G-IA2 suggests that the security parameters were robust. However, the security header was marked as "Unknown," which could indicate a potential issue in the message's integrity or encryption status. The lack of response from the UE to the AMF's security mode command is concerning, as it suggests that the UE may not have processed the command correctly or there was a failure in the communication process. According to the 3GPP standards, the UE should respond to such commands to ensure ongoing secure communication. The absence of a response could lead to vulnerabilities or indicate a failure in maintaining the expected security protocol. Therefore, based on the interaction and the lack of response from the UE, the action taken by the UE appears to be insecure. Insecure

242	242	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 03f3 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.11997199058532715 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.12023186683654785 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. Subsequently, the AMF sent a security mode command to the UE, which was protected, indicating that encryption and integrity protection were applied. The security mode command included parameters such as the ABBA value, cipher algorithm (128-5G-EA1), and integrity algorithm (128-5G-IA2). However, the UE did not provide a response to the security mode command. According to the 3GPP 5G standards, after the 5G-AKA process, the UE should respond to the security mode command to establish secure communication by agreeing on the ciphering and integrity protection algorithms. The absence of a response from the UE suggests a failure to complete the security setup, which is a critical step in ensuring secure communication. This lack of response could indicate a potential vulnerability or misconfiguration in the UE's handling of security procedures. Therefore, based on the 5G standard, the UE's action in this scenario is considered insecure, as it did not complete the necessary steps to secure the communication channel. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. Subsequently, the AMF sent a Security Mode Command to the UE. Notably, the Security Mode Command was sent as a plain NAS message, indicated by the security header being set to "Plain NAS message (0)." The UE, however, did not provide a response to this command. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The use of a plain NAS message for the Security Mode Command suggests a potential vulnerability, as it exposes the message to interception and tampering. The UE's lack of response could indicate a failure to proceed with the security mode setup, which is crucial for establishing secure communication. This lack of response might be due to the UE's detection of the insecure nature of the plain message, or it could be a malfunction or misconfiguration. Given the context, the UE's action of not responding to an unencrypted Security Mode Command aligns with maintaining security, as responding to such a message could compromise the integrity of the communication. Therefore, based on the 3GPP standards, the UE's action can be considered secure, as it avoided engaging in potentially insecure communication. Secure

244	244	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a security mode complete and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: security mode complete Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Plain ABBA: 0033 Cipher Algorithm: 5G-EA0 (null) Integrity Algorithm: 128-5G-IA2 Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.16002106666564941 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Security mode complete, Registration request 0.1602630615234375 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After the 5G Authentication and Key Agreement (5G-AKA) was completed, the UE sent a "security mode complete" message to the AMF, indicating that it accepted the security parameters. However, the AMF then sent a "security mode command" back to the UE as a plain message, which is unusual because, after the completion of 5G-AKA, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The ciphering algorithm used was 5G-EA0 (null), which means no encryption was applied, and the integrity algorithm was 128-5G-IA2. The security header was marked as a plain NAS message, which further indicates that the message was not encrypted. The UE did not respond to this plain security mode command, which could be interpreted as a failure to recognize or accept the insecure communication. According to the 3GPP standards, after the security mode command is accepted, all NAS messages should be encrypted and integrity protected. The fact that the UE did not respond to an unencrypted security mode command suggests that it adhered to the security requirements by not engaging in potentially insecure communication. Therefore, based on the 3GPP standards, the UE's action can be considered 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. The UE sent an authentication response to the AMF, which is a part of the 5G Authentication and Key Agreement (5G-AKA) process. However, the 5G-AKA was not completed, as indicated in the test summary. Following the authentication response, the AMF sent an identity request to the UE, specifically requesting the International Mobile Equipment Identity Software Version (IMEISV). Notably, this identity request was sent in plain text, as the encryption of messages is contingent upon the completion of the 5G-AKA process. The UE did not provide a response to the identity request. According to the 3GPP standards, the UE should not respond to identity requests sent in plain text when the 5G-AKA process is incomplete, as this could expose sensitive information. By not responding to the identity request, the UE adhered to secure communication practices, preventing potential exposure of its identity in an unencrypted format. Therefore, the UE's action in this scenario was aligned with the security protocols outlined by 3GPP, ensuring that sensitive information was not transmitted insecurely. Secure

246	246	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: TMSI UE provided: No response The packet capture during the test using wireshark is: 0.11967587471008301 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11993288993835449 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed during the NAS communication phase. After the UE sent an authentication response, the AMF issued an identity request to the UE. Notably, this identity request was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The AMF requested the Temporary Mobile Subscriber Identity (TMSI) from the UE, but the UE did not provide a response. According to the 3GPP standards, the 5G-AKA procedure must be completed to establish a secure communication channel, ensuring that subsequent messages are encrypted. The UE's lack of response to the identity request in plain text suggests a cautious approach, as responding to such requests without encryption could expose sensitive information. By not responding, the UE potentially avoided a security risk, adhering to the principle of not transmitting sensitive data over an unprotected channel. Therefore, the UE's action in this scenario aligns with secure communication practices as outlined by the 3GPP standards. Secure
247	247	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.1999650001525879 UE to AMF SACK (Ack=2, Arwnd=106496) , UplinkNASTransport, Authentication response 0.20019102096557617 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response, followed by the AMF sending an identity request. The identity request from the AMF was sent in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed. Since the 5G-AKA was not completed, the communication was not encrypted, and the AMF's request for the IMEISV was sent in plain text. The UE's lack of response to the identity request can be considered a secure action because it avoided transmitting sensitive information (IMEISV) over an unencrypted channel. This behavior aligns with the security principles of minimizing exposure of sensitive data when encryption is not in place. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response following the completion of the 5G Authentication and Key Agreement (5G-AKA) process. Subsequently, the AMF sent a security mode command to the UE, which was protected, indicating that encryption was applied to the message. The security mode command is a critical step in establishing secure communication, as it sets the ciphering and integrity protection algorithms for subsequent NAS messages. The AMF used the cipher algorithm 128-5G-EA2 and the integrity algorithm 128-5G-IA3, which are standard algorithms defined by 3GPP for secure communication. However, the UE did not provide a response to the security mode command, which is a deviation from the expected behavior. According to 3GPP standards, the UE should respond to the security mode command to confirm the establishment of security settings. The absence of a response from the UE suggests a failure to complete the security setup, leaving the communication potentially vulnerable. Therefore, based on the 3GPP standards, the UE's action in this scenario is considered insecure, as it did not adhere to the required protocol for establishing secure communication. Insecure
249	249	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 0.7274200916290283 UE to AMF UplinkNASTransport, Service request 0.7277319431304932 AMF to UE SACK (Ack=7, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with a configuration update command. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to this exchange, which is a prerequisite for establishing a secure communication channel. However, the configuration update command from the AMF was sent as a plain NAS message, indicated by the security header being set to "Plain NAS message (0)." This means that the message was not encrypted, despite the 5G-AKA completion, which should have enabled encryption for subsequent NAS messages. The UE did not provide any response to this plain message, which could be interpreted as a lack of action to secure the communication or a failure to recognize the security lapse. According to the 3GPP standards, after the 5G-AKA procedure, NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the UE did not respond to an unencrypted message suggests a potential security vulnerability, as it did not enforce the expected security measures. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario was insecure. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. The AMF's request was sent in plain text, asking for the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed. Since the 5G-AKA was not completed in this scenario, the communication was not encrypted, and the AMF's request was sent in plain text. The UE's lack of response to the identity request can be seen as a security measure, as it avoided sending sensitive information like the IMEISV over an unencrypted channel. This behavior aligns with the security principles of minimizing exposure of sensitive data when encryption is not in place. Therefore, the UE's action of not responding to the identity request in an unencrypted state is considered secure according to the 3GPP standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is crucial for establishing a secure communication channel. The AMF's identity request was sent in plain text, requesting the Temporary Mobile Subscriber Identity (TMSI) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, the 5G-AKA procedure must be completed to ensure that messages are encrypted and secure. Since the 5G-AKA was not completed, the communication was not encrypted, leaving the identity request vulnerable to interception. The UE's lack of response to the plain text identity request can be seen as a cautious action, as responding could have exposed sensitive information without the protection of encryption. Therefore, the UE's decision not to respond to the identity request in an unencrypted state aligns with maintaining security standards. In this context, the UE's action was secure, as it avoided transmitting potentially sensitive information over an insecure 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. Notably, the AMF's identity request was sent in plain text, and it requested the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed. Since the 5G-AKA was not completed, the communication was not encrypted, which is a potential security risk. The UE's lack of response to the plain text identity request can be seen as a cautious action, as responding to such requests without encryption could expose sensitive information. Therefore, the UE's decision not to respond to the identity request in plain text aligns with maintaining security standards by avoiding the transmission of sensitive information without encryption. Based on this analysis, the UE's action was secure. Secure
253	253	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: GUTI UE provided: No response The packet capture during the test using wireshark is: 0.7599589824676514 UE to AMF UplinkNASTransport, Service request 0.7601721286773682 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF issuing an identity request. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to this exchange, which is a prerequisite for ensuring that subsequent NAS messages are encrypted. However, the identity request from the AMF was sent in plain text, requesting the Globally Unique Temporary Identifier (GUTI) from the UE. The UE did not respond to this request. According to the 3GPP standards, after the 5G-AKA procedure, NAS messages should be encrypted to protect the integrity and confidentiality of the communication. The fact that the AMF sent an identity request in plain text could be considered a security vulnerability, as it exposes sensitive information. The UE's lack of response to the plain text identity request can be interpreted as a security-conscious action, as responding could have compromised its identity information. By not responding, the UE avoided potential exposure of its GUTI in an unprotected manner. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security as per the 3GPP standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. After the completion of the 5G Authentication and Key Agreement (5G-AKA), which is necessary for establishing a secure communication channel, the UE sent an uplink NAS transport message to the AMF. This message was followed by a downlink message from the AMF, which was a service accept message sent in plain text. Notably, the UE did not provide any response to this plain text message. According to the 3GPP standards, once the 5G-AKA is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent a plain text message indicates a potential security lapse, but since the focus is on the UE's actions, the critical point is the UE's lack of response to the unencrypted message. This lack of response suggests that the UE did not accept or process the insecure message, which aligns with secure behavior as per the 3GPP standards. Therefore, based on the UE's actions, the communication can be considered secure. Secure
255	255	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEI UE provided: No response The packet capture during the test using wireshark is: 12.160748958587646 UE to AMF InitialUEMessage, Service request, Service request [RRCEstablishmentCause=mo-Data] 12.161019086837769 AMF to UE SACK (Ack=19, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF issuing an identity request. The 5G Authentication and Key Agreement (5G-AKA) procedure was completed prior to this exchange, which is a prerequisite for ensuring that subsequent NAS messages are encrypted. However, the AMF sent the identity request in plain text, requesting the International Mobile Equipment Identity (IMEI) from the UE. The UE did not respond to this request. According to the 3GPP standards, after the 5G-AKA procedure, NAS messages should be encrypted to protect sensitive information such as the IMEI. The UE's lack of response to the plain text identity request can be interpreted as a security measure to avoid exposing its IMEI in an unencrypted format. This behavior aligns with the security principles outlined by 3GPP, which emphasize the protection of user identity and equipment information. Therefore, the UE's action of not responding to an unencrypted identity request is considered secure, as it prevents potential exposure of sensitive information. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "registration complete" message, followed by the AMF sending a "gmm status" message. Notably, the downlink message from the AMF was sent in plain text, and the 5GMM Cause was 97, which indicates a message type that is non-existent or not implemented. The UE did not provide a response to this message. According to the 3GPP standards, once the 5G Authentication and Key Agreement (5G-AKA) is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent a plain text message after the 5G-AKA process suggests a potential security vulnerability, as it exposes the communication to interception and tampering. The UE's lack of response to the plain text "gmm status" message could be interpreted as a security measure, as it did not engage with an unencrypted message that could be considered non-compliant with the expected security protocols. This behavior aligns with the 3GPP standards, which emphasize the importance of encrypted communication post-authentication. Therefore, the UE's action of not responding to the plain text message can be considered secure, as it avoided engaging in potentially insecure communication. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "registration complete" message, followed by the AMF sending an "identity request" message. Notably, the identity request from the AMF was sent in plain text, and it requested the Subscription Concealed Identifier (SUCI) from the UE. However, the UE did not respond to this request. According to the 3GPP standards, after the completion of the 5G Authentication and Key Agreement (5G-AKA), all NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. The fact that the AMF sent an identity request in plain text is a deviation from the expected secure communication protocol. The UE's lack of response to the plain text identity request can be interpreted as a security-conscious action, as responding to an unencrypted request could expose sensitive information. By not responding, the UE avoids potential exposure of the SUCI, which is a critical identifier that should be protected. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security as per the 3GPP standards. Secure

258	258	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Plain Security header: Integrity protected and ciphered (2) UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 2.4842751026153564 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session establishment request 2.4844861030578613 AMF to UE SACK (Ack=13, Arwnd=106401) , DownlinkNASTransport 2.688286066055298 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS message indicating "registration complete," which was acknowledged by the AMF. Subsequently, the AMF sent a deregistration request to the UE, which was transmitted in plain text but was integrity protected and ciphered, as indicated by the security header. The UE then responded with a deregistration request (UE originating) in an uplink NAS message. The fact that the AMF's deregistration request was sent in plain text raises concerns, as it suggests that the message was not encrypted, potentially exposing it to interception or tampering. However, the integrity protection and ciphering of the message provide a layer of security, ensuring that the message has not been altered and that its contents are confidential. The UE's response to the deregistration request was appropriate, as it followed the standard procedure by sending a deregistration request of its own. Based on the 3GPP standards, the UE's actions appear to be secure, as it adhered to the protocol by ensuring that messages were integrity protected and ciphered, even though the initial deregistration request from the AMF was in plain text. Therefore, the UE's communication can be considered secure. Secure
259	259	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Plain 5GMM Cause: 99 UE provided: No response The packet capture during the test using wireshark is: 0.5207638740539551 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.521324872970581 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Information element non-existent or not implemented) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. Subsequently, the AMF responded with a downlink NAS transport message containing a GMM status with a 5GMM Cause value of 99, indicating "Information element non-existent or not implemented." Notably, this downlink message was sent in plain text, which is unusual given that the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, suggesting that encryption should have been applied to NAS messages. The UE, however, did not provide any response to this plain-text message from the AMF. According to the 3GPP standards, once the 5G-AKA procedure is completed, NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the UE received a plain-text message and did not respond could indicate a lack of proper handling of unexpected or insecure messages, which is a potential security concern. The UE's lack of response might suggest it did not process the message due to its insecure nature, which could be a secure behavior. However, the absence of a response also leaves ambiguity about whether the UE recognized the security issue or simply failed to process the message. Given the context and the standards, the UE's action in this scenario appears insecure because it did not actively handle the receipt of an unencrypted message in a manner that clearly aligns with secure communication practices as outlined by 3GPP. Insecure

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, the UE initially completed the 5G Authentication and Key Agreement (5G-AKA) process, which is essential for establishing a secure communication channel. Following this, the UE sent a "registration complete" message to the AMF, indicating that it had successfully registered with the network. However, the AMF responded with a "gmm status" message in plain text, which is unusual because, after the 5G-AKA process, messages should be encrypted to ensure confidentiality and integrity. The "gmm status" message included a 5GMM cause code of 101, which typically indicates that the message is not compatible with the current protocol state. In response to this, the UE sent a "deregistration request," indicating that it chose to disconnect from the network. This action suggests that the UE detected an anomaly or inconsistency in the communication, likely due to the plain text message, and opted to terminate the session to protect itself from potential security threats. According to the 3GPP standards, the UE's decision to deregister in response to receiving an unencrypted message after the 5G-AKA process aligns with secure behavior, as it prevents further exposure to potential vulnerabilities. Therefore, the UE's actions in this scenario were consistent with maintaining security standards. Secure.
261	261	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a service request and then The AMF sent security mode command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: service request Subsequent Downlink message from the AMF: security mode command The downlink message from the AMF was sent as: Protected ABBA: 0101 Cipher Algorithm: 128-5G-EA1 Integrity Algorithm: 128-5G-IA2 Security header: Unknown UE provided: No response The packet capture during the test using wireshark is: 0.7511579990386963 UE to AMF UplinkNASTransport, Service request 0.7514059543609619 AMF to UE SACK (Ack=8, Arwnd=106496) , DownlinkNASTransport, Security mode command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with a security mode command. The 5G Authentication and Key Agreement (5G-AKA) process was completed, which is a prerequisite for secure communication. The AMF's downlink message, the security mode command, was sent as a protected message, indicating that encryption and integrity protection were applied. The ciphering algorithm used was 128-5G-EA1, and the integrity algorithm was 128-5G-IA2, both of which are standard algorithms for securing 5G communications. However, the security header was marked as unknown, and the UE did not provide a response to the security mode command. According to the 3GPP standards, after receiving a security mode command, the UE should respond with a security mode complete message to confirm the establishment of security contexts. The lack of response from the UE suggests a failure to complete the security procedure, which could leave the communication vulnerable to interception or tampering. Therefore, based on the 3GPP standards, the UE's action in this scenario was insecure, as it did not adhere to the expected protocol for establishing secure communication. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a service request, followed by the AMF responding with a security mode command. The 5G Authentication and Key Agreement (5G-AKA) process was completed, which is a prerequisite for secure communication. However, the security mode command from the AMF was sent as a plain message, with the security header indicating a plain NAS message (0). The ciphering algorithm used was 5G-EA0, which is a null algorithm, meaning no encryption was applied. The integrity algorithm was 128-5G-IA2, which provides integrity protection but not confidentiality. The UE did not respond to the security mode command. According to the 3GPP standards, after the 5G-AKA process, messages should be encrypted to ensure confidentiality and integrity. The use of a null cipher algorithm and the lack of encryption in the security mode command indicate a potential vulnerability, as the communication was not protected against eavesdropping. The UE's lack of response could suggest a failure to establish a secure connection or a refusal to proceed with insecure communication. Based on these observations, the UE's action in this scenario was insecure, as it did not ensure the confidentiality of the communication as per the 5G standard. Insecure
263	263	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent registration reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: registration reject The downlink message from the AMF was sent as: Plain 5GMM Cause: 74 UE provided: No response The packet capture during the test using wireshark is: 0.5198588371276855 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5200669765472412 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Registration reject (Temporarily not authorized for this SNPN) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. Following this, the AMF responded with a registration reject message, indicating that the UE was temporarily not authorized for the specified SNPN (Standalone Non-Public Network). Notably, the downlink message from the AMF was sent in plain text, which is a critical point of analysis. According to the 3GPP standards, once the 5G Authentication and Key Agreement (5G-AKA) procedure is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. However, in this test, the AMF's registration reject message was sent in plain text, which could potentially expose sensitive information if intercepted. The UE's lack of response to the registration reject message suggests that it did not take any further action, which might be appropriate given the rejection. However, the fact that the downlink message was not encrypted raises concerns about the security of the communication. Based on the 3GPP standards, the action taken by the UE in this scenario can be considered insecure due to the lack of encryption in the downlink message, which is a deviation from the expected secure communication practices post-5G-AKA. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS transport message to the AMF. However, the AMF responded with a registration reject message, citing an "Illegal ME" (Mobile Equipment) cause, which was sent in plain text. The 5GMM Cause code 6 typically indicates an issue related to the equipment being illegal or not allowed on the network. The UE did not provide any response to this rejection. According to the 3GPP standards, once the 5G-AKA is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. However, the AMF's registration reject message was sent in plain text, which is a deviation from the expected secure communication protocol. Despite the UE's lack of response, the fact that the AMF sent a plain text message after the 5G-AKA process suggests a potential vulnerability in the communication. The UE's actions, or lack thereof, do not directly indicate insecurity, but the overall interaction highlights a security concern due to the plain text message from the AMF. Therefore, while the UE's actions were not explicitly insecure, the test scenario reveals a potential security gap in the communication process. Insecure.

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending a service request. Subsequently, the AMF responded with an authentication request, which was sent in plain text. The authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI values. The UE then responded with an authentication failure message, indicating that the ngKSI was already in use. This sequence of events suggests that the UE detected a potential security issue, as the ngKSI (NAS key set identifier) was already associated with an existing security context, and the UE refused to proceed with the authentication process. According to the 3GPP 5G standards, the UE's response is considered secure because it prevents the reuse of an ngKSI that could potentially compromise the security context. By rejecting the authentication request due to the reuse of an ngKSI, the UE adheres to the security protocols designed to protect against replay attacks and ensure the integrity of the authentication process. Therefore, the UE's action in this scenario aligns with the security measures outlined by the 3GPP standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. Following this, the AMF responded with an authentication reject message. Notably, the downlink message from the AMF was sent in plain text, which is a critical point of analysis. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed successfully. In this scenario, although the 5G-AKA was marked as completed, the AMF's response was not encrypted, indicating a potential security lapse. The UE's lack of response to the plain-text authentication reject message suggests that it did not proceed with any further actions, which aligns with secure behavior as it did not engage with an unencrypted message that could be a security risk. The UE's decision to not respond to the plain-text message is consistent with maintaining security integrity, as engaging with unencrypted messages could expose it to vulnerabilities. Therefore, based on the 3GPP standards and the UE's cautious approach to the unencrypted message, the action taken by the UE can be considered secure. Secure

267	267	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a ul nas transport and then The AMF sent authentication reject to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: ul nas transport Subsequent Downlink message from the AMF: authentication reject The downlink message from the AMF was sent as: Plain UE provided: No response The packet capture during the test using wireshark is: 0.5199449062347412 UE to AMF SACK (Ack=4, Arwnd=106496) , UplinkNASTransport, UL NAS transport, PDU session establishment request 0.5201799869537354 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication reject This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an uplink NAS transport message, specifically a PDU session establishment request, to the AMF. Following this, the AMF responded with an authentication reject message. Notably, the downlink message from the AMF was sent in plain text, indicating that encryption was not applied. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed successfully. The test summary indicates that the 5G-AKA was completed, yet the AMF's response was unencrypted. The UE did not provide any response to the authentication reject message. In the context of 5G security, the lack of encryption in the AMF's message suggests a potential vulnerability, as sensitive information could be exposed. The UE's lack of response to an unencrypted authentication reject message could be seen as a cautious approach, avoiding further communication that might compromise security. However, the fact that the AMF's message was unencrypted after the 5G-AKA completion raises concerns about the security of the communication channel. Based on the 3GPP standards, the UE's action of not responding to an unencrypted message could be considered secure, as it avoids engaging in potentially insecure communication. However, the overall scenario highlights a security issue with the AMF's handling of encryption. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "registration complete" message, followed by the AMF sending a "configuration update command" as a downlink message. The 5G Authentication and Key Agreement (5G-AKA) process was completed prior to these exchanges, which is a prerequisite for ensuring that subsequent NAS messages are encrypted and protected. The packet capture indicates that the downlink message from the AMF was sent as "Protected," but the security header was marked as "Unknown," and the UE did not provide a response to the configuration update command. According to the 3GPP standards, after the 5G-AKA process, NAS messages should be encrypted and integrity protected to ensure secure communication. The lack of response from the UE could suggest a failure to process the message, possibly due to an issue with the security header or the message's integrity. This behavior raises concerns about the UE's ability to handle protected messages correctly, which is crucial for maintaining secure communication. Therefore, based on the observed interaction and the standards outlined by 3GPP, the action taken by the UE appears to be insecure. Insecure

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 the test scenario, the User Equipment (UE) completed the 5G Authentication and Key Agreement (5G-AKA) process, which is essential for establishing a secure communication channel. Following this, the UE sent a "registration complete" message to the Access and Mobility Management Function (AMF), indicating that it had successfully registered with the network. However, the AMF responded with a "deregistration accept" message, which was sent in plain text, meaning it was not encrypted. The UE did not provide any response to this message. According to the 3GPP standards, once the 5G-AKA process is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent a plain text message suggests a potential security vulnerability, as it could be intercepted or tampered with by an unauthorized entity. The UE's lack of response to the plain text message could indicate that it did not recognize the message as valid or secure, which aligns with the expected behavior of a secure UE. However, the absence of a response also leaves ambiguity about the UE's handling of the situation. Given the context, the UE's action of not responding to an unencrypted message can be seen as a cautious approach, but the overall interaction raises concerns about the security of the communication. Therefore, based on the 3GPP standards, the UE's communication in this scenario is deemed "Insecure."
270	270	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.03999805450439453 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.04024100303649902 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. The AMF's identity request was sent in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed first. Since the 5G-AKA was not completed, the communication remained unencrypted, which is a potential security risk. The UE's lack of response to the plain text identity request can be seen as a cautious action, as responding with sensitive information like the IMEISV in an unencrypted manner could expose the UE to security vulnerabilities. Therefore, the UE's decision not to respond to the identity request in plain text aligns with secure communication practices, as it avoids transmitting sensitive information without encryption. In conclusion, the UE's action was "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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. The AMF's identity request was sent in plain text, requesting the International Mobile Equipment Identity (IMEI) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed first. Since the 5G-AKA was not completed in this scenario, the communication was not encrypted, and the AMF's request was sent in plain text. The UE's lack of response to the plain text identity request can be considered a secure action. By not responding, the UE avoided transmitting sensitive information, such as the IMEI, over an unencrypted channel, which aligns with security best practices to protect user privacy and device identity. Therefore, the UE's action of not responding to the plain text identity request was secure according to the 5G standard outlined by 3GPP. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. The AMF responded with a service accept message, which was sent as a protected downlink message. However, it is important to note that the 5G Authentication and Key Agreement (5G-AKA) procedure was not completed at this point. The 5G-AKA is crucial for establishing a secure communication channel, as it ensures that messages are encrypted and authenticated. Without completing the 5G-AKA, the communication between the UE and the AMF remains unprotected, leaving it vulnerable to potential interception or tampering. Following the service accept message, the UE sent a deregistration request, indicating that it chose to terminate the session. The UE's decision to deregister could be seen as a precautionary measure, possibly due to the lack of completed authentication. However, the initial registration and subsequent deregistration occurred without the necessary security procedures being finalized, which is not in line with the 3GPP standards for secure communication. Therefore, the actions taken by the UE, in this case, were insecure due to the absence of completed 5G-AKA, which is essential for ensuring secure communication in 5G networks. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. The UE sent an authentication response to the AMF, which is a part of the 5G Authentication and Key Agreement (5G-AKA) process. However, before the 5G-AKA could be completed, the AMF sent a deregistration request to the UE. Notably, this deregistration request was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered. Despite this protection, the UE did not provide any response to the deregistration request. According to the 3GPP standards, for messages to be encrypted, the 5G-AKA process must be completed, which was not the case here. The UE's lack of response to the deregistration request could be seen as a failure to handle the situation securely, as it did not verify the integrity and authenticity of the message before acting upon it. This suggests a potential vulnerability, as the UE should ideally respond to or handle such requests only after successful authentication and key agreement. Therefore, based on the 3GPP standards and the incomplete 5G-AKA process, the UE's action in this scenario can be considered insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an authentication response after the initial NAS steps. Subsequently, the AMF sent a deregistration request to the UE. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure was not completed, which is crucial for establishing a secure communication channel. The deregistration request from the AMF was sent as a protected message with integrity protection, but since the 5G-AKA was not completed, the messages between the UE and AMF were not encrypted. The UE did not respond to the deregistration request. According to the 3GPP standards, the 5G-AKA procedure must be completed to ensure that messages are encrypted and integrity protected, providing confidentiality and protection against replay attacks. The lack of a response from the UE to the deregistration request could indicate that the UE did not accept the message due to the incomplete security setup. However, the fact that the UE sent an authentication response without the 5G-AKA being completed suggests a potential vulnerability, as the communication was not fully secure. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario can be considered insecure due to the incomplete security procedures. Insecure

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. This is a standard procedure where the UE attempts to register with the network. However, the AMF, which was under test control, responded with a deregistration request, indicating that the UE was to be terminated due to an "Illegal ME" (Mobile Equipment). Notably, this deregistration request was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered. However, the 5G Authentication and Key Agreement (5G-AKA) procedure, which is essential for establishing a secure communication channel, had not been completed at this point. The UE did not respond to the deregistration request. According to the 3GPP standards, the 5G-AKA procedure must be completed to ensure that messages are encrypted and integrity protected. Since the 5G-AKA was not completed, the UE's communication was not fully secure, as the initial registration request was sent without the necessary security context being established. The lack of response from the UE to the deregistration request could be seen as a failure to handle the situation securely, as it did not acknowledge or process the protected message. Therefore, based on the 3GPP standards and the sequence of events, the UE's actions in this scenario were insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending a security mode command. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure was not completed, which is crucial for establishing a secure communication channel. The security mode command from the AMF was sent as a plain NAS message, indicating that encryption was not applied to this message. The UE did not provide a response to the security mode command. According to the 3GPP standards, the 5G-AKA procedure must be completed before any NAS messages can be securely encrypted and integrity protected. Since the 5G-AKA was not completed, the UE's lack of response to the plain security mode command can be seen as a cautious action, as responding to an unencrypted command could expose sensitive information. Therefore, the UE's action of not responding to the plain security mode command aligns with maintaining security standards by avoiding potential vulnerabilities. In this context, the UE's behavior can be considered secure. Secure

277	277	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.04006814956665039 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040535926818847656 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the test scenario, the User Equipment (UE) engaged in NAS communication with the Access and Mobility Management Function (AMF). The UE sent an identity response message to the AMF, which was followed by the AMF sending a configuration update command back to the UE. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at this point, which is crucial for establishing a secure communication channel. The configuration update command from the AMF was sent with integrity protection, as indicated by the security header, but without encryption, since encryption requires the completion of the 5G-AKA process. The UE did not provide a response to the configuration update command. According to the 3GPP standards, the UE should not process or respond to configuration update commands that are not encrypted if the 5G-AKA has not been completed, as this could expose the UE to potential security risks. The lack of response from the UE suggests that it adhered to the security protocols by not engaging with a potentially insecure message. Therefore, based on the interaction and the standards outlined by 3GPP, the UE's action was secure. Secure
278	278	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.3110721111297607 UE to AMF UplinkNASTransport, Identity response 2.311551094055176 AMF to UE SACK (Ack=4, Arwnd=106496) , DownlinkNASTransport, Configuration update command 2.3115811347961426 UE to AMF SACK (Ack=3, Arwnd=106437) , UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) involved a sequence of NAS messages. The UE sent an identity response to the AMF, which was followed by the AMF sending a configuration update command back to the UE. Notably, this downlink message from the AMF was sent as a plain NAS message, meaning it was not encrypted. The UE did not respond to this configuration update command but instead sent a deregistration request, indicating that it chose to terminate the session. According to the 3GPP standards, for NAS messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed first. Since the 5G-AKA was not completed in this scenario, the messages remained unencrypted. The UE's decision to deregister upon receiving an unencrypted configuration update command suggests that it recognized the potential security risk of processing an unencrypted message and opted to terminate the session to prevent any security breach. This behavior aligns with secure practices, as it avoids processing potentially insecure commands. Therefore, the UE's action in this context can be considered secure. Secure

279	279	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007669925689697266 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. This uplink message was intended to initiate the registration process with the network. However, the AMF, which was under test control, responded with a deregistration accept message, effectively terminating the registration process. Notably, this downlink message from the AMF was sent as a protected message, but the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at this point. According to the 3GPP standards, the 5G-AKA procedure is crucial for establishing a secure communication channel, as it ensures mutual authentication and the derivation of encryption keys for protecting NAS messages. Since the 5G-AKA was not completed, the UE's communication was not encrypted, leaving it vulnerable to potential security threats. The UE did not respond to the deregistration accept message, which could indicate a lack of proper handling of unexpected or unauthorized messages. Given that the UE's actions did not adhere to the security protocols outlined by 3GPP, particularly the necessity of completing 5G-AKA before secure communication, the UE's behavior in this scenario can be considered insecure. Insecure
280	280	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent deregistration accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: deregistration accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007870197296142578 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. This uplink message was part of the Non-Access Stratum (NAS) communication, which is crucial for establishing a connection between the UE and the 5G core network. However, the subsequent downlink message from the AMF was a deregistration accept, which was sent as a protected message. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure, which is essential for securing NAS messages, had not been completed at this point. The UE did not respond to the deregistration accept message. According to the 3GPP standards, for NAS messages to be encrypted and secure, the 5G-AKA procedure must be completed first. Since the 5G-AKA was not completed, the UE's communication was not encrypted, leaving it vulnerable to potential security threats. The lack of response from the UE to the deregistration accept message could indicate a failure to recognize or process the message securely. Therefore, based on the 3GPP standards and the incomplete 5G-AKA, the action taken by the UE was insecure. Insecure

281	281	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered with new security context (4) UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.00080108642578125 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. Following this, the AMF responded with a configuration update command, which was sent as a protected message, specifically integrity protected and ciphered with a new security context. However, it is important to note that the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at the time of this interaction. According to the 3GPP standards, the 5G-AKA procedure is essential for establishing a secure communication channel, as it ensures that both integrity protection and encryption are based on a mutually authenticated security context. Since the 5G-AKA was not completed, the security context used for protecting the downlink message from the AMF was not fully established, which means the UE's lack of response could be due to its inability to verify the security context or authenticate the message properly. This lack of response from the UE suggests that it did not proceed with processing the message, potentially due to the absence of a valid security context, which aligns with secure behavior as per 3GPP standards. Therefore, the UE's action of not responding to the configuration update command without a completed 5G-AKA process can be considered secure, as it prevents the processing of potentially unauthenticated or improperly secured messages. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an initial registration request to the AMF. Subsequently, the AMF responded with a configuration update command, which was sent as a protected message with integrity protection and ciphering. However, the UE did not provide any response to this command. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed first. In this scenario, the 5G-AKA was not completed, which means that the security context necessary for encryption and integrity protection was not established. Despite the AMF sending a protected message, the lack of a completed 5G-AKA indicates that the UE did not have the necessary security context to securely process the message. The absence of a response from the UE could suggest that it did not accept the message due to the incomplete security setup, which aligns with secure behavior as per the 3GPP standards. Therefore, the UE's action of not responding to the configuration update command without a completed 5G-AKA can be considered secure, as it avoided processing potentially insecure messages. Secure

283	283	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006029605865478516 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In the test scenario, the User Equipment (UE) initiated communication with the Access and Mobility Management Function (AMF) by sending an initial registration request. This is a standard procedure in 5G networks where the UE attempts to register with the network. The AMF responded with a service accept message, which was sent as a protected downlink message. However, the 5G Authentication and Key Agreement (5G-AKA) procedure, which is crucial for establishing a secure communication channel, had not been completed at this point. The 5G-AKA is responsible for mutual authentication between the UE and the network and for deriving encryption keys to protect subsequent messages. Since the 5G-AKA was not completed, the UE's communication was not encrypted, leaving it vulnerable to potential interception or tampering. The UE did not respond to the service accept message, which could indicate a lack of proper handling of the situation where security procedures were not fully established. According to the 3GPP standards, the UE should ensure that the 5G-AKA is completed before engaging in protected communication to maintain security. Therefore, the action taken by the UE in this scenario was insecure, as it did not adhere to the necessary security protocols outlined by the 3GPP for secure communication. Insecure
284	284	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent service accept to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: service accept The downlink message from the AMF was sent as: Protected UE provided: Deregistration request (UE originating) The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0006928443908691406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Service accept 0.2013227939605713 UE to AMF UplinkNASTransport, Deregistration request (UE originating) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this test scenario, the User Equipment (UE) initiated communication with the Access and Mobility Management Function (AMF) by sending an initial registration request. The AMF responded with a service accept message, which was sent as a protected downlink message. However, the 5G Authentication and Key Agreement (5G-AKA) procedure, which is crucial for establishing a secure communication channel, was not completed. This means that the encryption and integrity protection of NAS messages, which rely on the successful completion of 5G-AKA, were not in place. Despite this, the UE proceeded to send a deregistration request, indicating that it was originating the deregistration process. The lack of completion of the 5G-AKA process suggests that the communication between the UE and the AMF was not fully secure, as the necessary cryptographic protections were not established. According to the 3GPP standards, the 5G-AKA procedure is essential for ensuring the confidentiality and integrity of messages exchanged between the UE and the network. Therefore, the action taken by the UE, in this case, can be considered insecure, as it did not adhere to the security protocols required for secure communication in a 5G standalone network. Insecure

285	285	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected and ciphered (2) UE provided: No response The packet capture during the test using wireshark is: 0.039772987365722656 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.039936065673828125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (PLMN not allowed) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending a deregistration request. The deregistration request was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered. However, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at the time of this interaction. According to the 3GPP standards, for messages to be securely encrypted, the 5G-AKA process must be completed to establish the necessary security context. Since the 5G-AKA was not completed, the security context required for encryption and integrity protection was not established. Despite the AMF sending a protected message, the UE did not respond, which could indicate that it did not recognize the security context or chose not to process the deregistration request without a valid security context. This lack of response from the UE suggests that it did not proceed with any action that could compromise its security, adhering to the 3GPP standards that require a completed 5G-AKA for secure communication. Therefore, the UE's action in not responding to the deregistration request without a valid security context can be considered secure. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. This uplink message was part of the Non-Access Stratum (NAS) communication, which is crucial for establishing a connection between the UE and the 5G core network. Following this, the AMF responded with a downlink message, specifically a GMM status message, which was sent as a protected message. However, the 5G-AKA (Authentication and Key Agreement) procedure had not been completed at this point, which is necessary for ensuring that messages are encrypted and secure. The GMM status message from the AMF included a 5GMM Cause value of 98, indicating that the message type was not compatible with the protocol state. The UE did not provide any response to this message. According to the 3GPP standards, the UE should not process or respond to messages that are not properly authenticated or encrypted, especially when the 5G-AKA procedure has not been completed. The lack of response from the UE suggests that it adhered to this security principle by not engaging with a potentially insecure message. Therefore, based on the 3GPP standards, the UE's action of not responding to the unverified message from the AMF was secure. Secure

287	287	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a initial registration request and then The AMF sent gmm status to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: initial registration request Subsequent Downlink message from the AMF: gmm status The downlink message from the AMF was sent as: Protected 5GMM Cause: 3 UE provided: No response The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.000408172607421875 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, 5GMM status (Illegal UE) This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. This uplink message was followed by a downlink message from the AMF, which was a GMM status message indicating an "Illegal UE" with a 5GMM Cause value of 3. Notably, this downlink message was sent as "Protected," but the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is necessary for encryption of NAS messages. The UE did not provide a response to the GMM status message. According to the 3GPP standards, the UE should not process or respond to messages that are not properly authenticated and encrypted, especially when the 5G-AKA procedure has not been completed. The lack of response from the UE suggests that it adhered to the security protocols by not engaging with a potentially insecure message. This behavior aligns with the 3GPP standards, which emphasize the importance of completing the 5G-AKA procedure before secure communication can occur. Therefore, the UE's action of not responding to the unverified message was appropriate and secure according to the 5G security standards. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) began with the UE sending an initial registration request. Following this, the AMF responded with a security mode command, which was sent as a protected message. The security mode command utilized the 5G-EA0 (null) ciphering algorithm and the 128-5G-IA2 integrity algorithm, with the security header indicating that the message was integrity protected with a new security context. However, the UE responded with a 5GMM status message indicating "Invalid mandatory information." This suggests that the UE did not process the security mode command correctly, potentially due to the lack of completion of the 5G Authentication and Key Agreement (5G-AKA) procedure, which is necessary for establishing a secure communication context. The use of the 5G-EA0 (null) ciphering algorithm means that no encryption was applied, which is acceptable only if the integrity protection is robust and the 5G-AKA procedure is completed. Since the 5G-AKA was not completed, the communication was not fully secure, as the integrity protection alone does not suffice without encryption in a new security context. Therefore, the UE's action in this scenario was insecure according to the 5G standard outlined by 3GPP. Insecure.

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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. Notably, the AMF's identity request was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is a prerequisite for encrypting NAS messages. The AMF requested the Globally Unique Temporary Identifier (GUTI) from the UE, but the UE did not provide a response. According to the 3GPP standards, the 5G-AKA procedure must be completed to ensure that NAS messages are encrypted, thereby protecting sensitive information such as the UE's identity. In this scenario, the UE's lack of response to the plain text identity request can be interpreted as a security measure to avoid exposing its identity without encryption. This behavior aligns with the security principles outlined by 3GPP, which emphasize the importance of protecting user identity and other sensitive information. Therefore, the UE's action of not responding to the plain text identity request can be considered secure, as it prevents potential exposure of sensitive information in an unprotected manner. Secure
290	290	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a identity response and then The AMF sent identity request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: identity response Subsequent Downlink message from the AMF: identity request The downlink message from the AMF was sent as: Plain Requested identity from the UE: IMEISV UE provided: No response The packet capture during the test using wireshark is: 0.039791107177734375 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response 0.040058135986328125 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Identity request This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. The AMF's identity request was sent in plain text, requesting the International Mobile Equipment Identity Software Version (IMEISV) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to ensure that messages between the UE and the AMF are encrypted, thereby securing the communication. In this scenario, since the 5G-AKA was not completed, the communication was not encrypted, and the AMF's request was sent in plain text. The UE's lack of response to the identity request can be interpreted as a security measure to avoid transmitting sensitive information over an unencrypted channel. This behavior aligns with the security principles outlined by 3GPP, which emphasize the importance of protecting user identity and sensitive information. Therefore, the UE's action of not responding to the identity request in an unencrypted state can be considered a secure practice in this context. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF sending an identity request. Notably, the AMF's identity request was sent in plain text, and it requested the Temporary Mobile Subscriber Identity (TMSI) from the UE. However, the UE did not provide a response to this request. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed first. Since the 5G-AKA was not completed in this scenario, the communication remained unencrypted. The UE's lack of response to the plain text identity request from the AMF can be considered a secure action. By not responding, the UE avoided potentially exposing sensitive information, such as the TMSI, over an unencrypted channel. This behavior aligns with security best practices, as it prevents the leakage of subscriber identity information in the absence of a secure communication channel. Therefore, the UE's action in this scenario was secure. Secure
292	292	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a authentication response and then The AMF sent deregistration request to the UE. The test summary as follows: 5G-AKA: Not completed yet Uplink message from the UE: authentication response Subsequent Downlink message from the AMF: deregistration request The downlink message from the AMF was sent as: Protected Security header: Integrity protected (1) UE provided: No response The packet capture during the test using wireshark is: 0.11100292205810547 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.11120295524597168 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (Not 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. The UE sent an authentication response to the AMF, which is a part of the 5G Authentication and Key Agreement (5G-AKA) process. However, before the 5G-AKA could be completed, the AMF sent a deregistration request to the UE. This deregistration request was integrity protected, as indicated by the security header, but the UE did not provide any response to this request. According to the 3GPP standards, for messages to be encrypted, the 5G-AKA process must be completed, which was not the case here. The lack of response from the UE to the deregistration request could be seen as a security measure, as the UE might be programmed to not respond to unexpected or potentially malicious requests, especially when the authentication process is incomplete. However, the fact that the UE did not respond at all could also indicate a lack of proper handling of such scenarios, which might be a security concern. Given that the UE did not engage further without a completed authentication process, it suggests a cautious approach, but the absence of a response mechanism might be a vulnerability. Therefore, based on the 3GPP standards and the observed behavior, the UE's action can be considered "Insecure" due to the lack of a defined response to the deregistration request.

293	293	This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent a registration complete and then The AMF sent configuration update command to the UE. The test summary as follows: 5G-AKA: Completed Uplink message from the UE: registration complete Subsequent Downlink message from the AMF: configuration update command The downlink message from the AMF was sent as: Plain Security header: Plain NAS message (0) UE provided: No response The packet capture during the test using wireshark is: 2.651521921157837 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originating) 2.65175199508667 AMF to UE SACK (Ack=13, Arwnd=106429) , DownlinkNASTransport, Configuration update command This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.	In this security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is crucial for establishing a secure communication channel. Following this, the UE sent an uplink NAS message indicating "registration complete." Subsequently, the AMF responded with a downlink NAS message, specifically a "configuration update command," which was sent as a plain NAS message without encryption. The security header indicated that it was a plain NAS message (0), and the UE did not provide any response to this message. According to the 3GPP standards, once the 5G-AKA process is completed, NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent a plain NAS message without encryption suggests a potential security vulnerability, as it exposes the communication to interception and tampering. The UE's lack of response to the plain message could be interpreted as a failure to adhere to security protocols, as it should ideally reject or request a secure message. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario appears to be insecure, as it did not ensure the confidentiality and integrity of the communication. Insecure
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: 3131313131313131005fb686550000 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. After the completion of the 5G Authentication and Key Agreement (5G-AKA), the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with secure communication. However, the subsequent message from the AMF, an "authentication request," was sent in plain text rather than being encrypted. This is a critical point because, according to the 3GPP standards, once the 5G-AKA is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The UE did not respond to the plain text authentication request, which suggests that it did not accept the insecure communication. This behavior aligns with the 3GPP standards, as the UE should not process unencrypted messages after security mode has been established. Therefore, the UE's action of not responding to the plain text message can be considered secure, as it adhered to the expected security protocols by not engaging in potentially insecure communication. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved the UE sending a "security mode complete" message after the 5G Authentication and Key Agreement (5G-AKA) process was completed. This indicates that the UE was ready to proceed with secure communication. However, the AMF responded with a "service reject" message, which was sent in plain text, indicating a protocol error with an unspecified cause (5GMM Cause: 111). The UE did not provide any response to this service reject message. According to the 3GPP standards, once the 5G-AKA is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent a plain text message after the security mode was completed suggests a potential vulnerability, as it exposes the communication to interception and manipulation. The UE's lack of response to the plain text service reject message could be seen as a failure to maintain secure communication, as it did not challenge or reject the unencrypted message. Therefore, based on the 3GPP standards, the UE's action in this scenario can be considered insecure, as it did not ensure that all subsequent communications were encrypted after the security mode was completed. Insecure
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 the test scenario, the User Equipment (UE) completed the 5G Authentication and Key Agreement (5G-AKA) process, which is essential for establishing a secure communication channel. Following this, the UE sent a "security mode complete" message to the Access and Mobility Management Function (AMF), indicating that it was ready to proceed with secure communication. However, the AMF then sent an "authentication request" message to the UE in plain text, which is unusual because, after the completion of 5G-AKA, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The UE did not respond to this plain-text authentication request, which suggests that it did not accept the insecure communication attempt. According to the 3GPP standards, the UE should expect encrypted messages after the security mode is established, and the lack of response from the UE indicates that it adhered to this expectation by not engaging with an unencrypted message. This behavior aligns with the security protocols outlined by 3GPP, as the UE did not compromise its security by responding to a potentially insecure message. Therefore, the action taken by the UE was secure. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) was observed. After completing the 5G Authentication and Key Agreement (5G-AKA), the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with secure communication. However, the subsequent message from the AMF was a "deregistration accept," which was sent in plain text, meaning it was not encrypted. The UE did not respond to this message. According to the 3GPP standards, once the 5G-AKA is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent a plain text message after the security mode was completed suggests a potential vulnerability, as the UE should have expected encrypted communication. The UE's lack of response to the plain text message could indicate that it did not accept the unencrypted message, which aligns with secure behavior. However, the test does not provide enough information to confirm whether the UE rejected the message due to its plain text nature or for another reason. Based on the available information, the UE's action of not responding to an unencrypted message after security mode completion suggests adherence to security protocols, but the lack of explicit rejection leaves some ambiguity. Therefore, the UE's behavior can be considered "Secure" in this context.
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved several key steps. Initially, the 5G Authentication and Key Agreement (5G-AKA) procedure was completed, which is a prerequisite for establishing a secure communication channel. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it was ready to proceed with secure communication. However, the AMF responded with an "authentication reject" message, which was sent in plain text. The UE did not provide any response to this message. According to the 3GPP standards, once the 5G-AKA procedure is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent an "authentication reject" message in plain text suggests a deviation from the expected secure communication protocol. However, the UE's lack of response to the plain text message can be interpreted as a secure action, as it did not proceed with any further communication that could compromise its security. By not responding, the UE avoided engaging in potentially insecure communication. Therefore, based on the 3GPP standards and the UE's actions, the UE's behavior can be considered secure. 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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After completing the 5G Authentication and Key Agreement (5G-AKA) process, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters and was ready for secure communication. However, the AMF responded with an "authentication reject" message, which was sent in plain text. According to the 3GPP standards, once the 5G-AKA process is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent an "authentication reject" message in plain text suggests a deviation from the expected secure communication protocol. The UE's lack of response to the plain text message could be interpreted as a failure to maintain secure communication, as it did not reject or challenge the unencrypted message. This behavior could potentially expose the UE to security vulnerabilities, as it did not adhere to the expected security measures outlined by the 3GPP standards. Therefore, based on the interaction and the standards, the action taken by the UE was insecure. Insecure
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 security test for a 5G standalone User Equipment (UE), the interaction between the UE and the Access and Mobility Management Function (AMF) involved a sequence of NAS (Non-Access Stratum) messages. After the completion of the 5G Authentication and Key Agreement (5G-AKA), the UE sent a "security mode complete" message to the AMF, indicating that it had successfully established a secure NAS connection. Subsequently, the AMF sent an "identity request" message to the UE, requesting the Temporary Mobile Subscriber Identity (TMSI). Notably, this identity request was sent in plain text, which is a critical point of concern. According to the 3GPP standards, once the security mode is complete, all subsequent NAS messages should be encrypted to protect the integrity and confidentiality of the communication. The UE, however, did not respond to the identity request, which could be interpreted as a security measure to avoid transmitting sensitive information over an unencrypted channel. This lack of response suggests that the UE adhered to the security protocols by not engaging in potentially insecure communication. Therefore, based on the 3GPP standards and the UE's decision to withhold a response to an unencrypted identity request, the action taken by the UE can be considered secure. Secure