

UE Response Evaluation Report: Test time: 2025-07-21 17:02:32

SL	Test Name	Test content	Remark
1	1	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, specifically requesting the International Mobile Equipment Identity (IMEI). Notably, this identity request was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed, meaning that the communication was not encrypted. The UE did not respond to the identity request. According to the 3GPP standards, the UE should not transmit sensitive information such as the IMEI in plain text, as this could expose the device to potential security threats. By not responding to the identity request sent in plain text, the UE adhered to the security protocols that aim to protect sensitive information until a secure communication channel is established. Therefore, the UE's action of not responding to the identity request in an unencrypted state aligns with the security expectations of the 5G standard. Secure</p>
2	2	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 identity request was sent in plain text, which is a standard procedure until encryption is established. However, the UE's action of responding to a plain text identity request with sensitive information like SUCI, without the protection of encryption, exposes it to potential security risks. This is because the SUCI is meant to protect the subscriber's permanent identifier (SUPI) and should ideally be transmitted securely. Therefore, based on the 3GPP standards and the lack of encryption due to the incomplete 5G-AKA, the UE's action in this scenario is considered insecure. Insecure</p>

3	3	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 threats that could arise from processing or acknowledging 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</p>
4	4	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 identity request was sent in plain text, which is a standard procedure until encryption is established. However, the UE's action of responding to a plain text identity request with sensitive information like the SUCI, without the protection of encryption, exposes it to potential security risks. This is because the SUCI is derived from the SUPI (Subscription Permanent Identifier) and should be protected to prevent tracking and interception by unauthorized entities. Therefore, based on the 3GPP standards and the lack of encryption due to the incomplete 5G-AKA, the UE's action of providing an identity response in this context is considered insecure. Insecure</p>

5	5	<p>This is 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:</p> <p>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)</p> <p>The packet capture during the test using wireshark is:  0.0 UE to AMF InitialUEMessage, 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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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) process 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</p>
6	6	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 its intention to terminate the registration process. According to the 3GPP standards, the 5G-AKA procedure is essential for establishing a secure communication channel by generating encryption keys. Since the 5G-AKA was not completed, the communication remained unencrypted, exposing the UE to potential security risks. The UE's action to deregister after receiving a plain-text rejection is a standard response, but the lack of encryption due to the incomplete 5G-AKA process makes the communication insecure. Therefore, while the UE's response was procedurally correct, the overall communication was insecure due to the absence of encryption. Insecure</p>

7	7	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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_TSC, with the ngKSI indicating a native security context. The UE responded with an authentication failure message, specifying that the non-5G authentication was unacceptable. 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. The UE's response to reject the authentication request due to its non-compliance with 5G standards demonstrates adherence to the security protocols outlined by 3GPP. By refusing to proceed with an insecure authentication process, the UE maintained the integrity and confidentiality of its communication. Therefore, the action taken by the UE was secure, as it correctly identified and rejected an authentication attempt that did not meet the necessary security requirements. Secure.</p>
---	---	---	--

8	8	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure was not completed, which is crucial for establishing a secure communication channel. The UE responded with a 5GMM status message indicating "Invalid mandatory information." This response suggests that the UE detected an issue with the received authentication request, possibly due to the lack of encryption or invalid parameters. According to the 3GPP standards, the 5G-AKA procedure must be completed to ensure that messages are encrypted and secure. Since the authentication request was sent in plain text and the 5G-AKA was not completed, the UE's response of invalid mandatory information indicates that it did not proceed with the authentication, which aligns with secure behavior as per the standards. The UE's action to not accept the plain text authentication request without completing the 5G-AKA process demonstrates adherence to security protocols. Therefore, the UE's actions in this scenario were secure. Secure</p>
---	---	--	---

9	9	<p>This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent an identity response and then the AMF sent identity request to the UE. The test summary as follows:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in its communication.</p>	<p>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 been completed, which is a prerequisite for encrypting NAS messages. The UE then responded with another identity response. According to the 3GPP standards, the exchange of sensitive information such as the Subscription Concealed Identifier (SUCI) should be protected by encryption to prevent interception and unauthorized access. Since the 5G-AKA was not completed, the communication was not encrypted, and the UE's response to a plain text identity request could potentially expose sensitive information. Therefore, the action taken by the UE in responding to an unencrypted identity request is considered insecure according to the 5G standard outlined by 3GPP.</p> <p>Insecure</p>
---	---	--	---

10	10	<p>This is 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:</p> <p>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: 3131313131313131006f90d2550000 AUTN: 35353535353535353535353535353535 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: Authentication failure (ngKSI already in use)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, as encryption of NAS messages requires the establishment of a security context through 5G-AKA. The AMF's authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI values. The UE responded with an authentication failure message, citing that the ngKSI (NAS key set identifier) was already in use. This response suggests that the UE detected a potential issue with the security context, as 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 ngKSI is a secure behavior, as it prevents the establishment of a compromised security context. By refusing to proceed with an already used ngKSI, the UE adheres to 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</p>
11	11	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 11, indicating "PLMN not allowed." 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 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 communication between the UE and the AMF was not encrypted, leaving it vulnerable to interception and potential tampering. The UE's action of sending an identity response without the completion of 5G-AKA means that sensitive information could be exposed. Therefore, based on the 3GPP standards, the UE's communication in this scenario was insecure. Insecure</p>

12	12	<p>This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent an identity response and then the AMF sent identity request to the UE. The test summary as follows:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in its communication.</p>	<p>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-related 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 potentially exposed. The UE's action of responding to an unencrypted identity request with sensitive information like the SUCI, without the protection of completed 5G-AKA, indicates a security vulnerability. Therefore, based on the 3GPP standards, the UE's action in this scenario was insecure. Insecure</p>
13	13	<p>This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent an identity response and then the AMF sent authentication reject to the UE. The test summary as follows:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in its communication.</p>	<p>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 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. 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. In this scenario, since the 5G-AKA was not completed, the communication remained unencrypted, leaving the UE vulnerable to security threats. The UE's lack of response to the plain-text authentication reject message further indicates a potential security oversight, as it did not attempt to reinitiate a secure authentication process. Based on the 3GPP standards, the UE's actions in this test were insecure, as it failed to ensure that the communication was encrypted and secure before proceeding with the NAS communication. Insecure</p>



14	14	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, this downlink message 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 crucial for establishing a secure communication channel, as it ensures that subsequent messages are encrypted. Since the 5G-AKA was not completed, the communication between the UE and AMF remained unencrypted, leaving the messages vulnerable to interception and potential tampering. The UE's action of sending an identity response without the completion of 5G-AKA, and thus without encryption, does not align with the security protocols outlined by 3GPP for secure communication. Therefore, the UE's communication in this scenario was insecure. Insecure</p>
15	15	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 message included parameters such as ABBA, RAND, AUTN, and ngKSI, but the AUTN was all zeros, which is not a valid authentication token. The UE responded with an authentication failure message, citing "Non-5G authentication unacceptable." This response indicates that the UE detected an anomaly in the authentication request, likely due to the invalid AUTN and the fact that the message was sent in plain text. According to the 3GPP standards, the UE is expected to reject any authentication attempts that do not comply with the 5G-AKA procedure, especially if the AUTN is invalid or if the message is not encrypted. Therefore, the UE's action to reject the authentication request was appropriate and aligned with the security protocols outlined by the 3GPP standards, ensuring that it did not proceed with an insecure authentication process. Secure.</p>

16	16	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, after the 5G-AKA process is completed, all 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 proceed with the security mode command due to its insecure transmission. This behavior aligns with the expectation that the UE should not accept or process unprotected messages after the security context is established. Therefore, the UE's action of not responding to the plain security mode command can be considered secure, as it adheres to the 3GPP standard of rejecting unprotected messages post-authentication. Secure</p>
17	17	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, instead of proceeding with the expected authentication completion, the AMF sent a service reject message back to the UE. Notably, this service reject message was sent in plain text, as the 5G-AKA process had not been completed, meaning that encryption had not yet been established. The 5GMM Cause code 111 indicates a "Protocol error, unspecified," which suggests an abnormal termination of the procedure. The UE did not provide any response to the service reject message. According to the 3GPP standards, the UE should not proceed with any sensitive operations or communications until the 5G-AKA process is completed and encryption is established. Since the UE did not respond to the plain text service reject message, it adhered to the security protocols by not engaging further without encryption. This behavior aligns with the security expectations of the 5G standard, as it prevents potential exposure of sensitive information. Therefore, the action taken by the UE was secure. Secure</p>

18	18	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 ensure that subsequent NAS messages are encrypted. In this scenario, 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 protection of encryption is considered insecure. This is because the SUCI, which is a sensitive identifier, should be protected to prevent potential interception and misuse. The UE should ideally not provide sensitive information like the SUCI in an unencrypted manner, as this could expose the UE to security vulnerabilities. Therefore, based on the 3GPP standards and the lack of encryption in this interaction, the action taken by the UE is deemed insecure. Insecure</p>
19	19	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 cipher algorithm (which is essentially a null cipher, meaning no encryption) 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. The UE's decision to reject the security mode command could be considered secure based on the 3GPP standards if the UE detected an anomaly or inconsistency in the security parameters, such as the use of the null cipher (5G-EA0), which does not provide encryption. The UE's rejection suggests a cautious approach to ensuring that the communication remains secure and that any potential vulnerabilities are not exploited. Therefore, the UE's action aligns with the security principles of the 5G standard, which prioritize the integrity and confidentiality of communications. Secure</p>

20	20	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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 an authentication request in plain text suggests that the security context was not established, and the UE's response to this unencrypted request could potentially expose sensitive information. Therefore, the UE's action of responding to an unencrypted authentication request without the completion of the 5G-AKA process is considered insecure, as it does not adhere to the security protocols outlined by the 3GPP for secure communication in 5G networks. Insecure</p>
----	----	--	--

21	21	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 messages. Initially, the UE sent an authentication response to the AMF. Subsequently, the AMF sent an authentication request back to the UE, which was transmitted in plain text. The UE then responded with an authentication failure message, citing a MAC (Message Authentication Code) failure. This sequence indicates that the UE detected an issue with the integrity of the authentication request, likely due to a mismatch in the expected MAC value, which is a critical component in ensuring message authenticity and integrity. According to the 3GPP 5G standards, the UE's response to a MAC failure is appropriate and aligns with the security protocols designed to protect against potential tampering or replay attacks. The UE's action to reject the authentication request due to a MAC failure demonstrates adherence to the security measures outlined in the 5G-AKA procedure, which is crucial for maintaining secure communication. Therefore, the UE's response can be considered secure as it correctly identified and reacted to a potential security threat.</p> <p>Secure</p>
----	----	---	---

22	22	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 to this plain authentication request with an authentication failure message, citing "Non-5G authentication unacceptable." This response indicates that the UE detected an anomaly in the authentication process, specifically the lack of encryption, and rejected the authentication attempt. This behavior aligns with the 3GPP standards, which emphasize the importance of secure and encrypted communication to protect against potential security threats. By rejecting the plain authentication request, the UE demonstrated adherence to security protocols, ensuring that only encrypted messages are accepted post-authentication. Therefore, the action taken by the UE was secure, as it correctly identified and responded to a potential security risk by refusing to proceed with an unencrypted authentication process. Secure</p>
----	----	---	---

23	23	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 UE's rejection of the security mode command suggests a cautious approach to ensuring the integrity and confidentiality of its communications, aligning with the security principles outlined by 3GPP. Therefore, the UE's action in this scenario can be considered secure, as it prioritized maintaining a secure communication environment by rejecting a potentially insecure configuration. Secure</p>
----	----	---	---

24	24	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 packet capture shows that the UE responded to the AMF's plain-text authentication request 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 encryption keys. The fact that the UE continued to communicate without the 5G-AKA being completed and responded to a plain-text authentication request suggests a potential vulnerability. The UE should ideally not proceed with sensitive exchanges until a secure context is established. Therefore, based on the 3GPP standards, the actions taken by the UE in this scenario appear to be insecure, as they do not adhere to the expected security protocols for ensuring encrypted communication. Insecure</p>
25	25	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 authentication reject message. The AMF's authentication reject message was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, which is necessary for encrypting messages. Upon receiving 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 secure response, as it prevents further communication with the network that could be potentially insecure due to the lack of encryption. The UE's decision to deregister helps mitigate any security risks associated with continuing communication in an unencrypted state. Therefore, the UE's actions align with the security protocols outlined by 3GPP, ensuring that it does not engage in potentially insecure communication. Secure</p>



26	26	<p>This is 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:</p> <p>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)</p> <p>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 (UE terminated) 0.15994787216186523 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) 0.3668229579925537 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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</p>
27	27	<p>This is 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:</p> <p>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)</p> <p>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 (UE terminated) 0.16001200675964355 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) 0.36782288551330566 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, 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 under the security protocols defined by the 3GPP standards. The UE's actions, including the acceptance of the deregistration request, were consistent with the expected behavior in a secure communication environment, as the messages were protected and the 5G-AKA was completed prior to these exchanges. Therefore, based on the adherence to the 3GPP security standards and the secure handling of messages, the UE's actions can be considered secure. Secure</p>

28	28	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 a "security mode complete" message to the AMF, indicating that it was ready to proceed with the security mode setup. 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, 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 5G-IA0 (null) integrity algorithm, which does not provide integrity protection. According to the 3GPP standards, the use of a null integrity algorithm is not secure, as it leaves the communication vulnerable to tampering. The UE's decision to reject the security mode command, therefore, aligns with the 3GPP standards, as it prevents the establishment of a potentially insecure communication channel. By rejecting the command, the UE ensures that it does not proceed with a security context that lacks proper integrity protection, thereby maintaining the security of the communication. Secure</p>
----	----	---	---

29	29	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 was ready to proceed with the security mode. However, the AMF subsequently sent a "security mode command" back to the UE, which was protected but used null ciphering 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 use of null algorithms (5G-EA0 and 5G-IA0) is generally considered insecure as it implies no encryption or integrity protection, which could expose the communication to potential interception or tampering. The UE's decision to reject the security mode command suggests that it identified the lack of adequate security measures and acted to prevent insecure communication. This behavior aligns with the 5G security standards, which prioritize the protection of user data and integrity. Therefore, the UE's action to reject the security mode command due to the use of null algorithms was a secure decision. Secure</p>
----	----	---	---

30	30	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 algorithms (5G-EA7 and 128-5G-IA2, respectively). 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 packet capture shows that the UE consistently responded with "security mode complete" messages, suggesting that it adhered to the security procedures by acknowledging the security mode command and maintaining the integrity of the communication. The use of integrity protection and the completion of the 5G-AKA process suggest that the UE's actions were in line with the 3GPP standards for secure communication. Therefore, based on the interaction and adherence to the security protocols, the UE's actions can be considered secure. Secure</p>
----	----	---	--

31	31	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In this test scenario, the interaction between the User Equipment (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 establishing a secure communication channel. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters. However, the AMF then sent a "security mode command" back to the UE, which was protected, suggesting that the AMF was attempting to renegotiate or confirm the security settings. The UE subsequently sent a "deregistration request," which was UE-originating, indicating that the UE decided to terminate its registration with the network. The use of the 5G-EA4 cipher algorithm for encryption and the 5G-IA0 (null) integrity algorithm is notable. The null integrity algorithm means that while the messages were encrypted, they were not integrity-protected, which could expose the communication to certain types of attacks, such as replay attacks. The security header indicated that the message was integrity protected with a new security context, but the use of a null integrity algorithm undermines this protection. Given these observations, the UE's actions appear insecure because the lack of integrity protection could compromise the security of the communication, despite the encryption. Therefore, based on the 3GPP 5G standards, the communication is deemed "Insecure."</p>
----	----	--	--

32	32	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 subsequently sent another "security mode command" to the UE, which was protected, as indicated by the security header being "integrity protected and ciphered." The UE did not respond to this subsequent command. The use of the cipher algorithm 5G-EA4 and integrity algorithm 128-5G-IA3 suggests that the communication was intended to be secure, adhering to the 3GPP standards for encryption and integrity protection. However, the lack of response from the UE to the second security mode command raises concerns. According to 3GPP standards, the UE should respond to security mode commands to ensure ongoing secure communication. The absence of a response could indicate a potential issue in the UE's handling of security procedures, which might expose it to vulnerabilities. Therefore, based on the UE's lack of response to the AMF's protected message, the action taken by the UE can be considered insecure. Insecure</p>
33	33	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 UE completed the 5G Authentication and Key Agreement (5G-AKA) process, which is crucial for ensuring that subsequent NAS (Non-Access Stratum) messages are encrypted. 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 responded with a "gmm status" message, which was protected, indicating that the message was encrypted. The 5GMM cause code of 6 corresponds to "Illegal ME," suggesting that the AMF identified the UE as an illegal mobile equipment. In response, the UE sent a "Deregistration request (UE originating)" message, which is a standard procedure when the UE decides to disconnect from the network, possibly due to the illegal ME status. The UE's action to deregister upon receiving a protected message with a cause indicating an issue aligns with the 3GPP standards, as it ensures that the UE does not continue to operate under potentially compromised conditions. The UE's decision to deregister can be seen as a secure action, as it prevents further communication that could be insecure or unauthorized. Therefore, based on the interaction and the adherence to the 3GPP standards, the UE's actions can be considered secure. Secure</p>

34	34	<p>This is 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:</p> <p>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)</p> <p>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) 0.360584020614624 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, indicating compliance with the deregistration request. The packet capture shows that the messages were exchanged with appropriate security headers, suggesting that the UE adhered to the security protocols outlined by the 3GPP standards. The use of integrity protection and encryption in the downlink message from the AMF, and the UE's subsequent response, demonstrate that the UE maintained secure communication throughout the interaction. Therefore, based on the adherence to the 5G security standards and the secure handling of messages, the action taken by the UE was secure. Secure</p>
35	35	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 UE sent an uplink message containing the "security mode complete" and "registration request," while the AMF responded with a downlink message containing the "service accept." The downlink message from the AMF was sent as "Protected," suggesting that encryption was applied, which aligns with the 5G security standards outlined by 3GPP. 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. Despite this, the initial actions taken by the UE, such as completing the 5G-AKA and sending the "security mode complete," suggest adherence to the security protocols required for encrypted communication. Therefore, based on the information provided and the completion of the 5G-AKA, the UE's actions appear to be secure according to the 3GPP standards, assuming the lack of response does not indicate a deeper issue. Secure</p>

36	36	<p>This is 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:</p> <p>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)</p> <p>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 (Unknown) 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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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), 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 integrity protected and ciphered, indicating that the message was secured according to the 5G security standards. The UE responded with a "deregistration accept" message, completing the deregistration process. 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. 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 was completed and the messages were protected, the actions taken by the UE appear to be secure according to the 5G standard outlined by 3GPP. Secure</p>
37	37	<p>This is 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:</p> <p>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)</p> <p>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 (Unknown) 0.5080060958862305 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Service accept 0.7117960453033447 UE to AMF UplinkNASTransport, Deregistration request (UE originating)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 uplink NAS transport message indicating a registration complete status. Following this, the AMF responded with a downlink NAS transport message, which included a service accept message. Notably, this downlink message was sent as protected, indicating 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. Subsequently, the UE sent a deregistration request, originating from the UE itself. The sequence of events suggests that the UE followed the expected protocol by first completing the 5G-AKA, which is necessary for secure communication, before engaging in further NAS messaging. The use of protected messages indicates adherence to the security standards outlined by 3GPP, as encryption is a critical component of secure communication in 5G networks. Therefore, based on the observed interaction and the completion of the 5G-AKA, the actions taken by the UE appear to be secure according to the 5G standard. Secure</p>



38	38	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 that the security header was "integrity protected with new security context." The ciphering algorithm used was 5G-EA0 (null), meaning no encryption was applied, while the integrity algorithm was 128-5G-IA2. Notably, the UE did not provide a response 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 context for subsequent communications. The lack of response from the UE suggests a failure to comply with the expected security procedures, leaving the communication potentially vulnerable. The use of a null cipher algorithm further indicates that the data was not encrypted, which is not secure for protecting sensitive information. Therefore, based on the 3GPP standards and the observed behavior, the action taken by the UE was insecure. Insecure</p>
39	39	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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," which was acknowledged by the AMF with a "configuration update command" in a downlink message. This downlink message was protected with a security header indicating that it was both integrity protected and ciphered, as per the 3GPP standards for secure communication. The UE responded with an "uplink NAS transport" message, confirming the "configuration update complete." The use of integrity protection and ciphering in the communication between the UE and the AMF suggests adherence to the security protocols outlined by 3GPP, ensuring that the messages were both authenticated and confidential. 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 5G standards. Therefore, based on the observed interaction and adherence to the security protocols, the UE's communication can be considered "Secure."</p>

40	40	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 3GPP standards. The process began with the completion of the 5G Authentication and Key Agreement (5G-AKA), 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 "configuration update command" back to the UE, which was protected with a security header indicating that the message was both integrity protected and ciphered. This ensures that the message was encrypted and authenticated, preventing unauthorized access or tampering. The UE then responded with a "configuration update complete" message, indicating successful receipt and processing of the command. The use of integrity protection and ciphering aligns with the 3GPP standards for secure communication, as it ensures that the messages are both confidential and authenticated. Given that the 5G-AKA was completed prior to these exchanges, the security context was established, allowing for secure NAS message exchanges. Therefore, based on the adherence to the 3GPP security standards and the successful protection of the messages, the actions taken by the UE can be considered secure. Secure</p>
----	----	---	---

41	41	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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) process 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. Instead, it sent an "InitialUEMessage" with a "Service request," which was followed by a "Service reject" from the AMF, stating 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 properly establish the security procedures as expected by the 3GPP standards. The UE's failure to respond to the security mode command and its subsequent actions indicate a potential security issue, as it did not adhere to the expected protocol for establishing a secure communication context. Therefore, based on the 3GPP standards, the UE's actions in this scenario can be considered insecure. Insecure</p>
42	42	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 AMF sent a series of messages, including a configuration update command and the deregistration accept message, after the UE's uplink NAS transport. 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 process the message correctly or that there was an issue with the message's integrity or confidentiality. According to the 3GPP standards, the UE should acknowledge such messages to ensure a secure and complete communication cycle. The absence of a response from the UE suggests a potential security vulnerability, as it may not have adhered to the expected protocol behavior. Therefore, based on the interaction observed, the UE's action appears to be insecure. Insecure</p>

43	43	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 an uplink NAS transport message, which was acknowledged by the AMF with a configuration update command. The AMF's downlink message was protected, as indicated by the security header being both integrity protected and ciphered. This suggests that the communication was encrypted, adhering to the security protocols outlined by the 3GPP standards. Subsequently, the UE sent a deregistration request, which was also part of the uplink NAS transport. The packet capture shows that the UE's messages were sent after the 5G-AKA was completed, ensuring that the communication was secure. The integrity protection and ciphering of the downlink message from the AMF further reinforce the security of the interaction. Based on the adherence to the 5G security standards and the completion of the 5G-AKA, the actions taken by the UE appear to be secure. Therefore, the communication between the UE and the AMF can be considered secure. Secure</p>
44	44	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 was followed by a deregistration request from the AMF. The deregistration request was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered. The UE responded appropriately by sending a deregistration accept message, indicating that it acknowledged the deregistration request. The fact that the 5G-AKA process was completed before these exchanges suggests that the security context was established, allowing for the encryption and integrity protection of NAS messages. The UE's response to the deregistration request was in line with the 3GPP standards, as it adhered to the security protocols by accepting the deregistration in a secure manner. The use of integrity protection and ciphering for the downlink message from the AMF further supports the secure handling of the communication. Therefore, based on the 3GPP standards and the observed interaction, the action taken by the UE was secure. Secure</p>

45	45	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 ensuring that subsequent NAS (Non-Access Stratum) 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 responded with a configuration update complete message. The packet capture from Wireshark confirms these exchanges, showing that the messages were transmitted in the expected sequence and with the necessary security protections in place. 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 adhered to the security requirements of the 5G standard. Therefore, the communication between the UE and the AMF can be considered secure. Secure.</p>
46	46	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 ensuring that subsequent NAS (Non-Access Stratum) 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 a security header indicating that the message was both integrity protected and ciphered. The UE then acknowledged this by sending a configuration update complete message back to the AMF. The packet capture confirms that the messages exchanged were appropriately protected, as the security header was set to ensure both integrity and confidentiality. This adherence to the 3GPP standards for secure communication in 5G networks suggests that the UE's actions were secure. The UE correctly followed the protocol by ensuring that the communication was protected after the 5G-AKA was completed, thus maintaining the confidentiality and integrity of the messages exchanged. Therefore, based on the interaction and the security measures observed, the UE's actions were in line with the 5G security standards. Secure.</p>

47	47	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 <del>ensuring that the</del> message was both integrity protected and ciphered. The UE then responded with a configuration update complete message. The packet capture from Wireshark confirms this sequence of events, showing that the messages were exchanged in a manner consistent with the 5G security protocols. 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. The integrity protection and ciphering of the messages ensure that the communication is both confidential and authentic, adhering to the security requirements outlined by the 3GPP for 5G networks. Therefore, based on the information provided and the adherence to the 5G security standards, the UE's communication can be considered secure. Secure</p>
----	----	---	---

48	48	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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-EA4 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 supported algorithms, an error in the security context, or other unspecified issues. According to the 3GPP standards, the UE's action to reject the security mode command can be considered secure if it detected a potential security risk or inconsistency in the proposed security parameters. By rejecting the security mode 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 potential security issue. Secure</p>
----	----	--	---

49	49	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. After the successful completion of the 5G Authentication and Key Agreement (5G-AKA), the UE initiated a service request to the AMF. In response, the AMF sent a Security Mode Command, which was protected, indicating that it was integrity protected with a new security context. The command specified the use of the 5G-EA0 ciphering algorithm (which is a null cipher, meaning no encryption) and the 128-5G-IA2 integrity algorithm. The UE, however, responded with a Security Mode Reject message, citing an unspecified reason for rejection. This rejection suggests that the UE did not accept the security parameters proposed by the AMF, possibly due to the use of the null ciphering algorithm, which does not provide encryption. According to the 3GPP standards, the use of a null cipher is generally not recommended for secure communication, as it leaves the data unencrypted. The UE's decision to reject the security mode could be interpreted as a precautionary measure to avoid operating under potentially insecure conditions. Therefore, the UE's action to reject the security mode command, given the use of a null cipher, aligns with maintaining a secure communication standard as per 3GPP guidelines. Secure</p>
50	50	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 essential for establishing a secure communication channel. Following this, the UE sent an uplink message, specifically a service request, 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 security protocols established after the 5G-AKA process. However, 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's message was protected aligns with these standards. However, the lack of response from the UE could be interpreted in different ways. It might suggest that the UE did not recognize or properly handle the deregistration accept message, which could be a security concern if it indicates a failure to process protected messages correctly. Alternatively, the lack of response could be a deliberate action by the UE, possibly due to the unexpected nature of the deregistration message following a service request. Without further context on the UE's internal decision-making process, it is challenging to definitively assess the security posture. However, given the scenario's setup and the UE's lack of response, which could imply a failure to handle the message appropriately, the action taken by the UE appears to be insecure according to the 3GPP standards. Insecure</p>



51	51	<p>This is 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:</p> <p>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)</p> <p>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) 25.85011601448059 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 this, the AMF sent a deregistration request to the UE, which was integrity protected and ciphered, 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.</p> <p>According to the 3GPP standards, the UE should only accept deregistration requests that are properly authenticated and encrypted, which seems to be the case here since the message was protected. (Message type not compatible with the protocol state)</p> <p>However, the test notes that the message type was not compatible with the protocol state, which could imply an unexpected or potentially malicious request. Despite this, the UE's response was in line with the protocol, as it accepted the deregistration in a secure manner, indicating that it adhered to the security requirements by ensuring the message was protected before responding. Therefore, based on the information provided and the adherence to the 3GPP standards, the UE's actions can be considered secure. Secure</p>
52	52	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 responded with a configuration update command. The downlink message from the AMF was protected, as indicated by the security header being both integrity protected and ciphered. This suggests that the communication was encrypted, adhering to the security protocols outlined by the 3GPP standards. Subsequently, the UE sent a deregistration request, which was also part of the uplink communication. The sequence of events indicates that the UE followed the expected security procedures by ensuring that the messages were protected after the 5G-AKA was completed. The use of integrity protection and ciphering for the downlink message further supports the notion that the communication was secure. Therefore, based on the 3GPP standards and the actions taken by the UE, the communication can be considered secure. Secure</p>

53	53	<p>This is 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:</p> <p>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)</p> <p>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) 17.204612970352173 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 messages (logged in the pcap file) that the UE adhered to the 5G security protocols by ensuring that the communication was protected after the 5G-AKA was completed. The integrity protection and ciphering of the downlink message from the AMF indicate that the communication was secure, as per the 3GPP standards. The UE's response to the deregistration request was appropriate and aligned with the expected behavior in a secure communication environment. Therefore, based on the interaction and adherence to the 5G security standards, the action taken by the UE was secure. Secure</p>
54	54	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, indicating that encryption was applied. The 5GMM Cause code of 100 suggests a conditional IE error, which typically indicates an issue with the information elements in the message. Notably, the UE did not provide a response to the AMF's GMM status message. 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's message was protected aligns with this requirement. However, the UE's lack of response could be seen as a failure to properly handle the GMM status message, which might indicate a potential issue in the UE's implementation of the 5G standard. The absence of a response could be due to the UE not recognizing the cause or an error in processing the protected message. While the initial encryption of the message was secure, the UE's failure to respond appropriately suggests a potential vulnerability in its handling of secure communications. Therefore, based on the UE's actions, the communication can be considered "Insecure."</p>

55	55	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 communications, had not been completed at this point. As a result, the messages exchanged were not encrypted. 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 communications are encrypted and secure. Since the UE did not respond to the plain-text authentication reject message, it adhered to the security protocols by not proceeding with an insecure communication. The lack of response from the UE indicates that it did not engage further in an unprotected exchange, which aligns with the security expectations of the 5G standard. Therefore, the action taken by the UE was secure. Secure</p>
56	56	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 test scenario, the 5G-AKA was not completed, and the AMF's authentication reject 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 a 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</p>

57	57	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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</p>
58	58	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 manipulation. 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 communication. 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 process. Insecure</p>

59	59	<p>This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent an initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 mutual authentication and the derivation of encryption keys for subsequent messages. 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 plain-text authentication reject message suggests that it did not proceed with any further actions that could compromise security. However, the initial registration request was sent without the protection of encryption, which is a security risk. Therefore, based on the 3GPP standards, the UE's action of sending an unencrypted registration request before completing the 5G-AKA procedure is considered insecure. Insecure</p>
60	60	<p>This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent an initial registration request and then The AMF sent authentication reject to the UE. The test summary as follows:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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</p>

61	61	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 "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 as it did not ensure the confidentiality and integrity of the communication. Insecure</p>
62	62	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 then 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 could be a point of concern. In a typical scenario, the UE should acknowledge such a message to complete the deregistration process securely. The absence of a response from the UE might suggest a potential issue in handling the message, which could be due to a security misconfiguration or a flaw in the UE's implementation. Therefore, while the AMF's action was secure, the UE's lack of response raises concerns about its compliance with the 3GPP security standards. In conclusion, the UE's behavior in this interaction is deemed "Insecure."</p>

63	63	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, indicating that the message was integrity protected and encrypted using the new security context established during the 5G-AKA. The security mode command included the ciphering algorithm 128-5G-EA1 and the integrity algorithm 128-5G-IA2, which are standard algorithms for securing NAS messages in 5G networks. The security header indicated that the message was integrity protected with a new security context, which is a crucial step in ensuring that subsequent communications are secure. After receiving the security mode command, the UE sent a deregistration request, which was UE-originating. This sequence of events suggests that the UE adhered to the 5G security procedures by first completing the 5G-AKA, ensuring that the subsequent messages were protected using the agreed-upon security algorithms. The UE's actions appear to be in line with the 3GPP standards for secure communication, as it responded appropriately to the security mode command and maintained the integrity and confidentiality of the communication. Therefore, based on the interaction and adherence to the 5G security standards, the UE's actions can be considered secure. Secure</p>
64	64	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 the UE's ability to handle encrypted communications as expected by the 5G security standards. This lack of response could be due to several reasons, such as an inability to decrypt the message, a failure in the integrity check, or an issue in the UE's protocol stack. Given that the UE did not respond to a protected message after the 5G-AKA was completed, this behavior is not aligned with the secure communication practices outlined by 3GPP for 5G networks. Therefore, the action taken by the UE in this scenario is considered insecure. Insecure</p>

65	65	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 secured communication. 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 potential vulnerabilities or misconfigurations. This cautious approach by the UE is consistent with maintaining a secure communication environment as per the 5G standards. Secure</p>
----	----	---	---



66	66	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 integrity protected, indicating that it was sent with a new security context using the specified cipher and integrity algorithms (128-5G-EA1 and 128-5G-IA2, respectively). However, the UE responded with a security mode reject message, citing an unspecified reason for rejection. This rejection suggests that the UE did not accept the security parameters or the context provided by the AMF, which could be due to a mismatch in expected security configurations or an issue with the integrity of the message. According to the 3GPP standards, the UE is expected to reject security mode commands if there is any inconsistency or if the integrity of the message cannot be verified. Therefore, the UE's action to reject the security mode command, despite being unspecified, aligns with the security protocols to prevent potential vulnerabilities or misconfigurations. This cautious approach by the UE ensures that it does not proceed with potentially insecure communication. Based on this analysis, the UE's action was secure. Secure</p>
----	----	---	---

67	67	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. In response, the AMF sent a protected downlink message containing a GMM status with a 5GMM Cause value of 98, which indicates "Message type not compatible with the protocol state." The UE then responded with an uplink message, also a GMM status, echoing the incompatibility of the message type with the protocol state. The sequence of events suggests that the UE correctly identified an inconsistency or unexpected message type from the AMF, which is a positive indication of its ability to detect and respond to protocol anomalies. According to the 3GPP standards, the UE is expected to handle such situations by either ignoring the message or responding with an appropriate status message, as it did. The UE's response demonstrates adherence to the protocol's security measures by not proceeding with potentially insecure or undefined operations. Therefore, based on the 5G standard outlined by 3GPP, the action taken by the UE was secure. Secure</p>
68	68	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 from Wireshark 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. Given that the 5G-AKA process was completed prior to these exchanges, the communication was encrypted, and the integrity protection was in place for the downlink message, the actions taken by the UE adhered to the security standards outlined by 3GPP for 5G networks. Therefore, the UE's communication can be considered secure. Secure</p>

69	69	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 accept a security configuration that might compromise the confidentiality of the communication. The UE's decision to reject the security mode command aligns with the principle of ensuring secure communication by not proceeding with a configuration that lacks encryption. Therefore, the UE's action was "Secure."</p>
----	----	---	--

70	70	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 an uplink message indicating "registration complete" to the AMF. Subsequently, the AMF responded with a downlink message, a "security mode command," which was sent as a protected message. The security mode command was intended to establish security settings, specifying the use of the 5G-EA0 (null) ciphering algorithm and the 128-5G-IA2 integrity algorithm. The security header indicated that the message was integrity protected and ciphered with a new security context. However, the UE did not provide any response to this command. According to the 3GPP standards, after receiving a security mode command, the UE is expected to respond appropriately to confirm the establishment of the security context. The lack of response from the UE suggests a failure to comply with the expected security procedures, which could potentially leave the communication vulnerable. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario was insecure. Insecure</p>
----	----	---	---

71	71	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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 the message was both integrity protected and ciphered. 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 128-5G-EA3 ciphering algorithm and the 5G-IA0 (null) integrity algorithm. However, the UE 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 confirm the security algorithms and proceed with secure communication. The lack of response from the UE suggests a failure to engage in the necessary security procedures, leaving the communication potentially vulnerable. Therefore, based on the 3GPP standards, the UE's action in this scenario is considered insecure. Insecure</p>
----	----	---	--

72	72	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 supported algorithms or a perceived security risk. According to the 3GPP standards, the UE's action to reject the security mode command can be considered secure if it detected a potential security issue or incompatibility, as it prevents the establishment of a potentially insecure communication channel. Therefore, the UE's decision to reject the security mode command, despite being unspecified, aligns with maintaining security integrity as per the 5G standards. Secure</p>
----	----	---	--

73	73	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 essential 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 the security mode configuration. However, the AMF responded with a "security mode command" message, 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 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 not recommended for secure communication, as it leaves the data unencrypted. The UE's decision to reject the security mode command, therefore, aligns with maintaining a secure communication standard by not accepting a potentially insecure configuration. Based on this analysis, the UE's action was secure, as it adhered to the 3GPP standards by rejecting a security mode that could compromise the integrity and confidentiality of the communication. Secure</p>
----	----	---	--

74	74	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 protective measure, possibly due to a perceived anomaly or inconsistency in the security parameters or context provided by the AMF. According to the 3GPP standards, the UE is expected to ensure that the security context is valid and that the integrity and confidentiality of the communication are maintained. By rejecting the security mode command, the UE may have been acting to prevent a potential security breach, such as a man-in-the-middle attack or a misconfiguration that could compromise the security of the communication. Therefore, the UE's action aligns with the 3GPP's emphasis on maintaining robust security measures, even if it results in rejecting a command from the network. Secure</p>
----	----	--	--



75	75	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 establish a secure communication context. The lack of response from the UE indicates a failure to complete the security procedure, leaving the communication potentially vulnerable. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario is considered insecure. Insecure</p>
76	76	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, and the AMF requested the Subscription Concealed Identifier (SUCI) from the UE. However, the UE did not provide any response to this request. According to the 3GPP standards, the 5G-AKA (Authentication and Key Agreement) procedure must be completed before any NAS messages can be encrypted. Since the 5G-AKA was not completed, the messages remained unencrypted. The UE's lack of response to the identity request, which was sent in plain text, suggests a cautious approach to avoid exposing sensitive information like the SUCI without proper encryption. This behavior aligns with security best practices, as responding to an unencrypted identity request could potentially expose sensitive subscriber information. Therefore, the UE's action of not responding to the plain text identity request can be considered secure according to the 5G standard. Secure</p>

77	77	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 identity request was sent in plain text, which is a standard procedure until encryption is established. However, the UE's action of responding to a plain text identity request with sensitive information like the SUCI, without the protection of encryption, exposes it to potential security risks. This is because the SUCI is meant to protect the subscriber's permanent identifier (SUPI) and should ideally be transmitted securely. Therefore, based on the 3GPP standards and the lack of encryption due to the incomplete 5G-AKA, the UE's action in this scenario is considered insecure. Insecure</p>
78	78	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 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, specifying that the security mode was rejected for unspecified reasons. This sequence of events suggests that the UE detected an issue with 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 use of a null cipher algorithm is generally not secure for protecting data confidentiality. 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 could compromise data confidentiality. Secure</p>

79	79	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 use of the 5G-EA0 (null) cipher algorithm means that no encryption was applied, which is a potential security concern as it leaves the communication unencrypted. The UE's decision to reject the security mode command could be interpreted as a protective measure against an insecure configuration, as the lack of encryption could expose sensitive information. According to the 3GPP standards, the UE should ensure that both integrity and confidentiality are maintained in communications. By rejecting the security mode command that proposed a null cipher, the UE acted in accordance with security best practices to prevent unencrypted communication. Therefore, the action taken by the UE was secure. Secure</p>
80	80	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 configuration update command, which was sent as a protected message with a security header indicating integrity protection with a new security context. This implies 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 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 protocol states or an unexpected message type. According to the 3GPP standards, the UE should be able to handle such messages appropriately if they are sent within a valid security context. The fact that the UE flagged the message as incompatible suggests a potential issue in the protocol handling or state management, which could be a security concern if it leads to denial of service or other vulnerabilities. Therefore, while the initial setup of the secure channel was correct, the UE's handling of the subsequent message raises concerns about its robustness in maintaining secure communication as per the 5G standard. In this context, the action taken by the UE appears to be insecure. Insecure</p>

81	81	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 integrity protected, 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 a 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 security settings for subsequent communications. 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 securing NAS communications in 5G networks, which require the establishment of encryption and integrity protection to safeguard the data exchanged between the UE and the network. Insecure</p>
----	----	--	---

82	82	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 the message was encrypted and integrity protected. The security mode command specified the use of 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. However, the UE responded with a security mode reject message, citing an unspecified reason for the rejection. The UE's rejection of the security mode command could be due to several factors, such as a mismatch in the expected security algorithms or an issue with the security context. According to the 3GPP standards, the UE is expected to reject a security mode command if it detects any inconsistencies or potential security vulnerabilities in the proposed security parameters. By rejecting the security mode command, the UE is potentially preventing the establishment of a compromised security context, which aligns with the security principles outlined by 3GPP. Therefore, the UE's action to reject the security mode command, despite being unspecified, can be considered a cautious and secure response to ensure the integrity and confidentiality of its communication. Secure</p>
83	83	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 summary 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 UE sent an "InitialUEMessage" with a "Service request," and the AMF responded with a "DownlinkNASTransport" containing a "Service accept" message, 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 could indicate a failure to properly handle the protected message, which may suggest a potential security issue or a malfunction in the UE's handling of encrypted communications. Given that the UE did not respond to a protected message after the 5G-AKA was completed, this behavior could be considered insecure as it does not align with the expected secure communication flow outlined by the 3GPP standards. Therefore, based on the interaction observed, the UE's action was "Insecure."</p>

84	84	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 downlink 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 perceived anomaly or inconsistency in the security parameters or context provided by the AMF. According to the 3GPP standards, the UE is expected to ensure the integrity and authenticity of the messages it receives, and it has the right to reject a security mode command if it detects any issues. Therefore, the UE's action to reject the command, despite the lack of a specified reason, aligns with the security principles of the 5G standard, as it prioritizes maintaining a secure communication environment. Based on this analysis, the UE's action can be considered "Secure."</p>
----	----	--	---

85	85	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 essential for establishing a secure communication context. Following this, the UE sent a "security mode complete" message to the AMF, indicating its readiness to proceed with the security mode settings. However, the AMF responded with a "security mode command," which was protected, suggesting that it was sent with integrity protection using a new security context. The UE then responded with a "security mode reject" message, citing an unspecified reason for rejection. The use of the 5G-EA0 (null) cipher and 5G-IA0 (null) integrity algorithms indicates that no encryption or integrity protection was applied, which is typically not secure for actual data transmission. The UE's rejection of the security mode command could be interpreted as a protective measure against an insecure configuration, as the null algorithms do not provide confidentiality or integrity. According to the 3GPP standards, the UE should reject security configurations that do not meet the required security levels. Therefore, the UE's action to reject the security mode command, given the use of null algorithms, aligns with maintaining security standards. Secure</p>
----	----	---	--

86	86	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 and ciphered (2)." The UE responded again with a "security mode complete" message. The use of the 128-5G-EA1 ciphering algorithm and the 128-5G-IA2 integrity algorithm suggests that the communication was encrypted and integrity-protected, adhering to the 3GPP standards for secure communication. The packet capture shows that the messages were acknowledged and transported securely, with the ABBA parameter being used as part of the security context. Given that the UE followed the expected protocol by completing the 5G-AKA and responding appropriately to the security mode command with protected messages, the actions taken by the UE appear to be secure according to the 5G standard. Therefore, the UE's communication can be considered "Secure."</p>
----	----	---	--



87	87	<p>This is 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:</p> <p>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)</p> <p>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  0.9985220432281494 AMF to UE DownlinkNASTransport, Service reject (UE identity cannot be derived by the network)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 encrypted and authenticated. However, the UE's subsequent response included a 5GMM status message indicating "Invalid mandatory information," which suggests that the UE did not correctly process the deregistration request. This response was followed by another service request from the UE, which was rejected by the AMF due to the inability to derive the UE's identity. The UE's action of sending a 5GMM status message with invalid information and then attempting to reinitiate a service request without addressing the deregistration request indicates a potential flaw in handling the AMF's message. According to the 3GPP standards, the UE should correctly interpret and respond to deregistration requests, especially when they are protected. The failure to do so, coupled with the invalid information provided, suggests a lack of adherence to the expected security protocols. Therefore, the UE's actions in this scenario can be considered insecure. Insecure</p>
88	88	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 authentication response to the AMF, which is a standard step in the 5G-AKA (Authentication and Key Agreement) process. 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, and ideally, such identity requests should be encrypted to prevent exposure of sensitive information. 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</p>

89	89	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 ensure that subsequent NAS messages are encrypted. 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 sensitive information, such as the SUCI, to potential interception. This is contrary to the security principles outlined by 3GPP, which emphasize the importance of protecting subscriber identity and ensuring secure communication. Therefore, the UE's action in this scenario is considered insecure. Insecure</p>
90	90	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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. In this scenario, the 5G-AKA was not completed, which means that the communication was not encrypted. The fact that the AMF sent an identity request in plain text and the UE responded with an identity response without encryption raises security concerns. The SUCI is a sensitive piece of information that should be protected to prevent potential interception and misuse. Since the 5G-AKA was not completed, the UE's response to the identity request was not secure, as it exposed sensitive information without encryption. Therefore, based on the 3GPP standards, the action taken by the UE was insecure. Insecure</p>

91	91	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 downlink message was protected, as it was both integrity protected and ciphered, adhering to the security protocols expected in 5G communication. However, the UE's subsequent response was a 5GMM status message indicating "Invalid mandatory information." This suggests that the UE did not handle the deregistration request appropriately, potentially due to a misinterpretation or mishandling of the protected message. According to the 3GPP standards, the UE should correctly interpret and respond to such messages, especially when they are integrity protected and ciphered. The UE's response indicating invalid information suggests a failure in processing the message securely, which could expose vulnerabilities in real-world scenarios. Therefore, based on the 3GPP standards and the observed behavior, the action taken by the UE was insecure. Insecure</p>
92	92	<p>This is 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:</p> <p>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)</p> <p>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) (Unprotected) 1.0037281513214111 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, which was integrity protected and ciphered, indicating that the message was encrypted and authenticated as per the 5G security standards. The UE then responded with a deregistration accept message, 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. The use of integrity protection and ciphering for the downlink message from the AMF indicates compliance with the 3GPP standards for secure communication. The UE's response to the deregistration request was appropriate and secure, as it followed the expected protocol by acknowledging the request with a deregistration accept message. This behavior aligns with the security requirements outlined by 3GPP, ensuring that the communication was conducted securely. Therefore, based on the interaction and adherence to the 5G security standards, the action taken by the UE was secure. Secure</p>

93	93	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 security mode. Subsequently, the AMF sent a "security mode command" to the UE, which was protected, indicating that the message was encrypted and integrity protected. The security context used a cipher algorithm (5G-EA4) and a null integrity algorithm (5G-IA0), which means no integrity protection was applied. The UE responded with a "security mode reject" due to a mismatch in security capabilities, suggesting that the UE detected a discrepancy between its security capabilities and the security requirements specified by the AMF. This action by the UE is consistent with the 3GPP standards, which require the UE to reject security mode commands if there is a mismatch in security capabilities, thereby preventing potential security vulnerabilities. By rejecting the security mode command, the UE ensured that it did not proceed with a potentially insecure configuration. Therefore, the action taken by the UE was secure according to the 5G standard outlined by 3GPP. Secure</p>
94	94	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 identity request was sent in plain text, which is a standard procedure in the initial stages of registration. However, the UE's action of responding to a plain text identity request with sensitive information like SUCI, without the protection of encryption, raises security concerns. The SUCI is designed to protect the subscriber's permanent identifier (SUPI) and should ideally be transmitted securely. Given that the UE provided an identity response without the completion of 5G-AKA, this action could potentially expose sensitive information, making the communication insecure. Therefore, based on the 3GPP standards and the lack of encryption due to the incomplete 5G-AKA, the UE's action in this scenario is deemed insecure. Insecure</p>

95	95	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, under controlled test conditions, responded with a deregistration request, which was integrity protected and ciphered, indicating that the message was encrypted and authenticated. The UE then responded with a deregistration accept message. The sequence of events suggests that the UE adhered to the 5G security protocols by ensuring that the communication was protected after the 5G-AKA was completed. The UE's response to the deregistration request, despite the message type being noted as not compatible with the protocol state, indicates that it followed the protocol by acknowledging the deregistration in a secure manner. The integrity protection and ciphering of the downlink message from the AMF further imply that the communication was secure. Based on the 3GPP standards, the UE's actions appear to be secure as it maintained the integrity and confidentiality of the communication throughout the interaction. Therefore, the UE's communication can be considered "Secure."</p>
96	96	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 NAS messages are encrypted. 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. Therefore, based on the 3GPP standards, the UE's action of responding to an unencrypted identity request without completing the 5G-AKA procedure is considered insecure. Insecure</p>

97	97	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 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 messages were exchanged in plain text, which exposes the communication to potential interception and eavesdropping. The UE's action of responding to an identity request sent in plain text without the protection of encryption is considered insecure according to the 3GPP standards, as it could lead to the exposure of sensitive information. Therefore, the UE's communication in this scenario was insecure. Insecure</p>
98	98	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, indicating that it was integrity protected with a new security context, as per the 5G-AKA procedure, which had been completed prior to this exchange. 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 in the protocol state, which could be a security measure to prevent processing potentially malicious or erroneous messages. According to the 3GPP standards, the UE should maintain protocol state integrity and reject messages that do not align with the expected state. The UE's action to send a 5GMM status message in response to an incompatible message type demonstrates adherence to these security principles, as it did not process the configuration update command that was not compatible with its current protocol state. Therefore, the UE's response can be considered secure as it aligns with the 5G standard's security requirements to protect against protocol state inconsistencies. Secure</p>

99	99	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 protected suggests that the encryption was in place. However, the UE's lack of response to the service accept message raises concerns about its ability to handle the protected message properly. This could indicate a potential issue with the UE's implementation of the security protocols, as it should have acknowledged the service accept message if it was processed correctly. Therefore, while the initial setup for secure communication was established, the UE's failure to respond appropriately suggests a lapse in secure communication handling. Insecure.</p>
100	100	<p>This is 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:</p> <p>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</p> <p>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 PDU session establishment)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, which implies that the 5G Authentication and Key Agreement (5G-AKA) procedure was completed successfully, ensuring that the messages were encrypted. However, the UE did not provide a response to the "gmm status" message. According to the 3GPP standards, the UE should respond appropriately to status messages to maintain a secure and synchronized communication state. The lack of response from the UE could indicate a potential issue in handling the status message, which might lead to vulnerabilities if not addressed. The security of the UE's actions is questionable because, while the initial communication was protected, the absence of a response to the status message could be seen as a deviation from expected behavior, potentially exposing the session to risks. Therefore, based on the 3GPP standards and the observed behavior, the UE's action in this scenario is considered "Insecure."</p>

101	101	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In the security test for the 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 encrypted and integrity protected, using the cipher algorithm 128-5G-EA3 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 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 complete the security procedure, which could leave the communication vulnerable to interception or tampering. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario is considered insecure. Insecure</p>
-----	-----	---	--



102	102	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 downlink message. The security mode command was transmitted using 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 5G standard outlined by 3GPP, 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 indicates that it recognized the lack of proper security measures and did not proceed with the communication under these conditions. This behavior aligns with the expectation that the UE should not accept insecure configurations. Therefore, the action taken by the UE can be considered secure, as it adhered to the security standards by not accepting a security mode command that did not provide adequate protection. Secure</p>
103	103	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 deregistration request, which was integrity protected and ciphered, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had been completed successfully, as encryption and integrity protection are only possible post-authentication. The UE, however, did not provide any response to the deregistration request. In the context of 3GPP standards, the lack of response from the UE could be seen as a security concern, as it did not acknowledge or process the deregistration request, which is a critical message indicating the termination of the session. This could imply a potential vulnerability or misconfiguration in the UE's handling of secure messages, as it should ideally respond to such requests to ensure proper session management and security compliance. Therefore, based on the interaction and the UE's lack of response to a protected message, the action taken by the UE appears to be insecure according to the 3GPP standards for secure communication in 5G networks. Insecure</p>

104	104	<p>This is 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:</p> <p>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</p> <p>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 (UE terminated) 0.5201320648193359 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (LAbbunot responsible)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 back 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 responsible for such requests to maintain a secure and synchronized state with the network. The lack of response from the UE could potentially indicate a security vulnerability, as it may lead to an unsynchronized state or leave the UE in an undefined state, which could be exploited. Therefore, while the initial communication was secure due to the protection and encryption of messages, the UE's failure to respond to the deregistration request suggests a lapse in maintaining secure communication as per the 3GPP standards. Insecure.</p>
105	105	<p>This is 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:</p> <p>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</p> <p>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 (UE terminated) 0.5614829063415527 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Configuration update command 0.7653870582580566 UE to AMF UplinkNASTransport, Configuration update complete</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 ensuring that subsequent NAS (Non-Access Stratum) 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 the message was both integrity protected and ciphered. The UE then acknowledged this with a configuration update complete message. 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, 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."</p>

106	106	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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-EA4 and the integrity algorithm 128-5G-IA3. 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 acted in accordance with the 5G security standards, ensuring that it did not proceed with a potentially insecure configuration. Therefore, the action taken by the UE was secure. Secure</p>
107	107	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, Registration complete" message to the AMF, indicating that it had completed the registration process. Subsequently, the AMF, under controlled test conditions, sent a "DownlinkNASTransport, Deregistration request" to the UE, which was integrity protected and ciphered, ensuring that the message was both encrypted and authenticated. The UE responded with an "UplinkNASTransport, Deregistration accept," acknowledging the deregistration request. 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, which was also part of the test scenario, indicates that it followed the expected protocol behavior by accepting the deregistration. Given that the communication was protected and the UE acted in accordance with the expected security procedures, the actions taken by the UE can be considered secure according to the 5G standard. Secure</p>

108	108	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, 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 encrypted and authenticated. 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 security measure to prevent processing potentially malicious or erroneous messages. According to the 3GPP standards, the UE's response to reject or flag an incompatible message type is a secure behavior, as it prevents the UE from acting on potentially harmful instructions. Therefore, the UE's action in this scenario aligns with the security protocols outlined by 3GPP, ensuring that only valid and expected messages are processed. Secure.</p>
109	109	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. Subsequently, the AMF responded with a "5GMM Status" message, which was protected, indicating that encryption was applied. The 5GMM cause code 98 suggests that the message type was not compatible with the protocol state, which the UE acknowledged by sending a "5GMM Status" message back to the AMF. This response from the UE indicates that it correctly identified the incompatibility of the message type with the current protocol state, as per the 3GPP standards. The UE's action to send a status message back to the AMF, acknowledging the issue, demonstrates adherence to the protocol's error handling procedures. Given that the communication was encrypted and the UE correctly handled the protocol state mismatch, the UE's actions can be considered secure according to the 5G standard outlined by 3GPP. Secure</p>

110	110	<p>This is 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:</p> <p>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</p> <p>The packet capture during the test using wireshark is: 0.5881869792938232 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originated) 0.5883810520172119 AMF to UE SACK (Ack=6, Arwnd=106429) , DownlinkNASTransport, 5GMM status (Message not compatible with the protocol state)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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), which is crucial 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. Subsequently, the AMF responded with a "gmm status" message, which was protected, meaning it was encrypted as per the 5G security protocols. The 5GMM Cause code 101 indicates that the message was not compatible with the protocol state, suggesting a potential issue or misalignment in the expected communication sequence. Notably, the UE did not provide a response to this message. According to the 3GPP standards, the UE should ideally respond to such messages to maintain a secure and synchronized communication state. The lack of response from the UE could imply a vulnerability or a failure to adhere to the expected protocol behavior, potentially leaving the communication channel in an insecure state. Therefore, based on the interaction and the UE's lack of response to the AMF's protected message, the action taken by the UE appears to be insecure. Insecure</p>
111	111	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 had been completed, allowing for encrypted communication. The AMF used the cipher algorithm 5G-EA5 and the integrity algorithm 5G-IA0 (null), 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 response suggests that the UE detected a discrepancy between its security capabilities and the security parameters proposed by the AMF. According to the 3GPP 5G standards, the UE is expected to reject security mode commands that do not align with its capabilities to prevent potential vulnerabilities or misconfigurations. By rejecting the security mode command due to a capabilities mismatch, the UE acted in accordance with the standard's security protocols, ensuring that it did not proceed with a potentially insecure configuration. Therefore, the action taken by the UE was secure. Secure</p>

112	112	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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.</p>
-----	-----	--	--

113	113	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 service request to the AMF. In response, the AMF issued a security mode command, which was protected using the cipher algorithm 128-5G-EA1 and the integrity algorithm 128-5G-IA2, with the 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 is expected to accept the security mode command if it is valid and properly protected. The rejection of the security mode command by the UE, especially with an unspecified reason, suggests a potential issue in the security negotiation process. This could indicate a misconfiguration, an incompatibility, or a security concern that the UE detected, leading it to reject the command to prevent potential vulnerabilities. Without further context on the reason for rejection, it is challenging to definitively assess the security posture. However, the UE's action to reject the command could be seen as a precautionary measure to maintain security integrity, assuming the rejection was due to a legitimate concern. Therefore, based on the information provided, the UE's action appears to be cautious and aligned with maintaining security standards, albeit with limited information on the specific cause of rejection. Secure</p>
114	114	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 with a configuration update complete message. 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 the confidentiality and integrity of the messages exchanged. 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 provided information and the adherence to the security protocols, the UE's communication can be considered "Secure."</p>

115	115	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, allowing for secure communication. The AMF used the cipher algorithm 5G-EA4 and the integrity algorithm 128-5G-IA3, with the security header indicating integrity protection with a new security context. However, the UE responded with a 5GMM status message indicating "Invalid mandatory information." This response suggests that the UE did not correctly process the security mode command, potentially due to an issue with the mandatory information required for the security context. According to the 3GPP standards, the UE should correctly interpret and respond to security mode commands to ensure secure communication. The presence of "Invalid mandatory information" indicates a failure in this process, which could lead to vulnerabilities in the security context. Therefore, based on the 3GPP standards, the action taken by the UE was insecure, as it failed to maintain the integrity and confidentiality expected in a secure 5G communication. Insecure</p>
-----	-----	---	---



116	116	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 (3). 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 could 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 suggests 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</p>
-----	-----	--	---

117	117	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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. This downlink message was protected, indicating that it was both integrity protected and ciphered with a new security context, using the specified cipher and integrity algorithms (5G-EA5 and 128-5G-IA1, respectively). However, the UE did not provide a 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 a secure communication context. The lack of response from the UE suggests a failure to complete the security procedure, which is critical for ensuring the confidentiality and integrity of subsequent communications. Therefore, based on the 3GPP standards, the UE's action in this scenario is considered insecure, as it did not adhere to the expected protocol for establishing a secure communication channel. Insecure</p>
118	118	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 ensuring that subsequent NAS (Non-Access Stratum) 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. This downlink message was protected with a security header indicating that it was both integrity protected and ciphered, as denoted by the security header type (2). The UE then acknowledged this by sending a configuration update complete message back to the AMF. The use of encryption and integrity protection in the communication between the UE and the AMF aligns with the security standards outlined by 3GPP for 5G networks, ensuring that the messages are secure from eavesdropping and tampering. Given that the 5G-AKA was completed and the messages were appropriately protected, the actions taken by the UE were secure according to the 5G standard. Therefore, the communication can be considered "Secure."</p>

119	119	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 context. 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 the rejection. This rejection suggests that the UE did not accept the security parameters proposed by the AMF, possibly due to the use of the null ciphering algorithm, which does not provide encryption. According to the 3GPP standards, the use of a null ciphering algorithm (5G-EA0) is generally considered insecure as it does not encrypt the data, leaving it vulnerable to interception. The UE's decision to reject the security mode command could be interpreted as a protective measure to avoid operating under insecure conditions. Therefore, the UE's action to reject the security mode command, given the proposed use of a null ciphering algorithm, aligns with maintaining secure communication standards. Secure.</p>
120	120	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 test indicates that the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is a prerequisite for ensuring that subsequent NAS messages are encrypted and protected. The packet capture shows that the "deregistration accept" message from the AMF was sent as a protected message, suggesting that encryption was applied as per the 5G security standards. However, the UE did not provide any response to the "deregistration accept" message. According to the 3GPP standards, the UE should ideally respond to such messages to confirm receipt and maintain a secure communication channel. The lack of response from the UE could indicate a potential issue in the communication process, as it may not be handling the deregistration process as expected. This could be seen as a security concern because it leaves the communication session in an uncertain state, potentially exposing the UE to vulnerabilities. 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</p>

121	121	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 Authentication and Key Agreement (5G-AKA) procedure was not completed, 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 are encrypted, thereby protecting the integrity and confidentiality of the communication. Since the 5G-AKA was not completed, the messages exchanged were not encrypted, leaving the communication vulnerable to interception and tampering. The UE's lack of response to the service reject message further indicates that it did not take any additional steps to secure the communication or to reinstate the authentication process. Based on the 3GPP standards, the UE's actions in this scenario were insecure, as it did not ensure the completion of the 5G-AKA process before proceeding with communication, resulting in unprotected message exchanges. Insecure.</p>
122	122	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 with the network. However, the AMF responded with a service reject message, indicating that the UE's identity could not be derived by the network. Notably, this downlink message was sent in plain text, as the 5G Authentication and Key Agreement (5G-AKA) procedure had not yet been completed. The 5G-AKA is essential for establishing a secure communication channel, as it ensures that messages are encrypted and authenticated. Since the UE did not provide any response to the service reject message, it adhered to the expected behavior when faced with a service reject due to identity issues. According to the 3GPP standards, the UE should not proceed with further communication if the network cannot derive its identity, especially when messages are not encrypted. Therefore, the UE's action of not responding further was in line with maintaining security, as it avoided potential exposure of sensitive information over an unencrypted channel. Based on this analysis, the UE's behavior was secure according to the 5G standard outlined by 3GPP. Secure</p>

123	123	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 UE sent an identity response, the AMF issued a security mode command, which was protected and included parameters such as the ABBA value, cipher algorithm (5G-EA4), and integrity algorithm (128-5G-IA1). The security header indicated that the message was integrity protected with a new security context. However, the UE responded with a security mode reject, citing an unspecified reason. 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 could be seen as a precautionary measure, as it did not proceed with the security mode setup without a completed 5G-AKA, which is crucial for ensuring secure communication. This cautious approach aligns with the 5G security standards, as it prevents the establishment of a potentially insecure connection. Therefore, the UE's action to reject the security mode command without a completed 5G-AKA was secure and in compliance with the 3GPP standards. Secure</p>
124	124	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In this test scenario, the interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) involved the exchange of identity-related 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 been completed, meaning that the communication was not yet encrypted. 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 used to protect the subscriber's identity. However, since the 5G-AKA procedure was not completed, the communication was not encrypted, leaving the identity information potentially exposed 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, is not aligned with the security expectations of the 5G standard. Therefore, the UE's action in this scenario can be considered insecure, as it did not ensure the confidentiality of the identity information. Insecure</p>

125	125	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, which is a prerequisite for encrypting NAS messages. 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 actions or communications 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 prevents any further communication that could potentially be insecure due to the absence of encryption. Therefore, the UE's action of not responding to the authentication reject message is consistent with maintaining security as per the 5G standard. Secure</p>
126	126	<p>This is 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:</p> <p>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)</p> <p>The packet capture during the test using wireshark is: 0.5059909820556641 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, UL NAS transport, PDU session established with QoS 0.5062329769134521 AMF to UE SACK (Ack=6, Arwnd=106401) , DownlinkNASTransport, Deregistration request (UE terminated) (Integrity) 0.7099969387054443 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 integrity protected and ciphered, indicating that the message was secured according to the 5G security standards. The UE responded with a "deregistration accept" message, completing the deregistration process. The use of integrity protection and ciphering in the downlink message from the AMF suggests that the communication was conducted securely, as per the 3GPP standards, which require that NAS messages be protected to ensure confidentiality and integrity. 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 exchanged under the protection of the established security context. Therefore, based on the interaction and adherence to the 5G security protocols, the actions taken by the UE can be considered secure. Secure</p>

127	127	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 the situation where messages are received in plain text. Based on the 3GPP standards, the action taken by the UE in this scenario is considered insecure, as it did not ensure the confidentiality and integrity of the communication. Therefore, the UE's communication in this test was "Insecure."</p>
128	128	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In this test scenario, the interaction between the User Equipment (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 a critical point to consider. According to the 3GPP standards for 5G, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to establish a secure communication channel, ensuring that subsequent messages are encrypted. However, in this test, the 5G-AKA was not completed, and the AMF sent the authentication request without encryption. The UE responded with a 5GMM status message indicating "Invalid mandatory information," which suggests that the UE detected an anomaly or non-compliance with expected security procedures. The UE's response indicates that it did not proceed with the authentication process due to the lack of encryption, which aligns with the security protocols outlined by 3GPP. This behavior demonstrates that the UE adhered to the security standards by not accepting an unencrypted authentication request, thereby preventing potential security vulnerabilities. Therefore, the action taken by the UE was secure according to the 5G standard. Secure</p>

129	129	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 downlink message, indicating that it was integrity protected with a new security context, using the 128-5G-IA2 integrity algorithm and the 5G-EA0 (null) cipher algorithm. 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 issue with the integrity protection. According to the 3GPP standards, the UE is expected to ensure that the security parameters are correctly negotiated and that the integrity and confidentiality of the communication are maintained. By rejecting the security mode command, the UE may have been acting to prevent a potential security breach, such as accepting a security context that does not meet the required standards. Therefore, the UE's action can be considered secure, as it prioritized maintaining the integrity and security of the communication over proceeding with potentially compromised parameters. Secure.</p>
-----	-----	--	---



130	130	<p>This is 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:</p> <p>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)</p> <p>The packet capture during the test using wireshark is:  0.04801797866821289 UE to AMF SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Identity response  0.0482211129760742 AMF to UE SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request  0.25036191940307617 UE to AMF UplinkNASTransport, Authentication failure (Non-5G authentication unacceptable)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 notable because, according to the 3GPP standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to establish a secure context for encrypting messages. The UE responded with an authentication failure, citing "Non-5G authentication unacceptable," indicating that it did not accept the authentication request as valid under the 5G security framework. This response suggests that the UE correctly identified the lack of a secure context, as the 5G-AKA was not completed, and the authentication request was not encrypted. The UE's action aligns with the 3GPP standards, which emphasize the importance of completing the 5G-AKA to ensure secure communication. By rejecting the authentication request due to its non-compliance with 5G security requirements, the UE demonstrated adherence to the security protocols designed to protect against potential vulnerabilities. Therefore, the UE's action was secure. Secure</p>
131	131	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, 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) process had not been completed. According to the 3GPP standards, the 5G-AKA process is crucial for establishing a secure communication channel, as it ensures that messages are encrypted and it vulnerable to interception and potential tampering. The UE did not provide any response to the registration reject message, which is consistent with the expected behavior when receiving such a message. However, the lack of encryption due to the incomplete 5G-AKA process indicates that the UE's communication was not secure according to the 5G standards. Therefore, the action taken by the UE in this scenario was insecure. Insecure</p>

132	132	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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 5GMM Cause code 99 indicates that the service reject was due to "Information element non-existent or not implemented." The UE did not provide any response to the service reject message. According to the 3GPP standards, the security of NAS messages relies on the completion of the 5G-AKA procedure to ensure encryption and integrity protection. Since the 5G-AKA was not completed, the communication remained unencrypted, leaving it vulnerable to potential interception or tampering. The UE's action of sending an identity response without the security context established by 5G-AKA could be considered insecure, as it exposes sensitive information without the protection of encryption. Therefore, based on the 3GPP standards, the UE's communication in this scenario was insecure. Insecure</p>
133	133	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 indicated by the absence of encryption, which is expected since the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed. The AMF's message included parameters such as ABBA, RAND, AUTN, and ngKSI values. The UE responded with an authentication failure message, specifying "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 an invalid authentication vector, and rejected it as per the 3GPP standards. The UE's action to reject the authentication request aligns with the security protocols outlined by 3GPP, which emphasize the importance of completing the 5G-AKA procedure to establish a secure context before proceeding with encrypted communication. By refusing to proceed with an authentication request that did not meet the 5G security standards, the UE demonstrated adherence to the security protocols designed to protect against potential vulnerabilities. Therefore, the action taken by the UE was secure. Secure</p>

134	134	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 an "Illegal UE" with a 5GMM Cause value of 3. 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, 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 remained unencrypted, leaving it vulnerable to security threats. The UE's action of sending an identity response without the completion of 5G-AKA, and thus without encryption, does not align with the security protocols outlined by 3GPP for secure communication. Therefore, the UE's communication in this scenario was insecure. Insecure</p>
135	135	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, 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. According to the 3GPP standards, the UE's action to reject the security mode command is appropriate and secure, as the security context was not adequately established due to the lack of encryption and integrity protection. The UE's rejection helps prevent potential vulnerabilities that could arise from operating under an insecure security context. Therefore, the UE's action was in line with maintaining secure communication standards as outlined by 3GPP. Secure</p>

136	136	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In this test scenario, the interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) involved the UE sending an identity response, followed by the AMF issuing a security mode command. The security mode command was sent as a protected message, with the ABBA value set to 3000, using the 5G-EA0 (null) ciphering algorithm and the 128-5G-IA3 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 5G standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed before secure communication can be established, ensuring that both encryption and integrity protection are properly set up. In this case, the 5G-AKA was not completed, and the ciphering algorithm used was 5G-EA0, which is a null algorithm providing no encryption. The UE's decision to reject the security mode command can be considered secure because it did not proceed with a potentially insecure configuration where encryption was not applied, and the integrity protection was based on an incomplete security context. By rejecting the security mode command, the UE avoided engaging in a communication session that could have been vulnerable to interception or tampering. Therefore, the UE's action aligns with maintaining security as per the 5G standards. Secure</p>
-----	-----	---	---

137	137	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 authentication request back to the UE. Notably, the AMF's authentication request 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's subsequent action was to send 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, and the UE's response to this unencrypted request could potentially expose sensitive information. Therefore, the UE's action of responding to an unencrypted authentication request without the completion of the 5G-AKA process is considered insecure, as it does not adhere to the security protocols intended to protect the integrity and confidentiality of the communication. Insecure</p>
-----	-----	--	---

138	138	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 that the communication adhered to the security protocols outlined by the 3GPP standards, which require that messages be protected to prevent unauthorized access and tampering. The UE's actions, in this case, appear to be secure as it followed the expected protocol by responding appropriately to a protected deregistration request. The integrity protection and encryption of the message indicate that the communication was secure, maintaining confidentiality and integrity as per the 5G security standards. Therefore, based on the interaction and adherence to the 3GPP security protocols, the UE's actions can be considered "Secure."</p>
-----	-----	--	---

139	139	<p>This is 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:</p> <p>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: 31303030000000007894d5bccd550000  AUTN: 00000000000000000000000000000000  ngKSI_TSC: Native security context  ngKSI_KSI: 7  UE provided: 5GMM status (Invalid mandatory information)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI values. However, the UE responded with a 5GMM status message indicating "Invalid mandatory information." This 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. 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. Since the 5G-AKA was not completed, the communication remained unencrypted and vulnerable to interception or tampering. The UE's response of "Invalid mandatory information" indicates that it did not proceed with the authentication process, which is a secure action given the circumstances. By not accepting the plain text authentication request, the UE adhered to security protocols that prevent unauthorized access and potential security breaches. Therefore, the UE's action in this scenario was secure, as it avoided proceeding with an insecure authentication process. Secure</p>
-----	-----	---	---

140	140	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. The authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI values. However, the UE did not proceed with the 5G Authentication and Key Agreement (5G-AKA) process, which is crucial for establishing a secure communication channel. Instead, the UE responded with a deregistration request, indicating that it chose to terminate the session rather than proceed with an insecure authentication process. According to the 3GPP standards, the 5G-AKA procedure must be completed to ensure that subsequent messages are encrypted and secure. By not completing the 5G-AKA and opting to deregister, the UE avoided engaging in potentially insecure communication, as the authentication request was sent in plain text, which could be vulnerable to interception or tampering. Therefore, the UE's decision to deregister rather than proceed with an insecure authentication process aligns with maintaining security standards. In this context, the UE's action can be considered secure, as it avoided engaging in a potentially insecure communication session. Secure</p>
141	141	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. The UE did not provide any response to the authentication reject message. 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 encryption keys. Since the 5G-AKA was not completed, the communication remained unencrypted, leaving it vulnerable to interception and manipulation. 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. However, the fact that the communication was not encrypted due to the incomplete 5G-AKA process indicates a potential security risk. Therefore, based on the 3GPP standards, the UE's communication in this scenario can be considered "Insecure."</p>



142	142	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 messages. Initially, the UE sent an authentication response to the AMF. Subsequently, the AMF sent an authentication request back to the UE, but notably, this message was sent in plain text, as indicated by the test summary. The UE then responded with an authentication failure message, citing "Non-5G authentication unacceptable." This sequence of events suggests that the UE detected an anomaly in the authentication process, specifically the lack of encryption in the AMF's authentication request. According to the 5G standard outlined by 3GPP, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed to establish a secure communication context, which includes encryption of messages. The UE's decision to reject the authentication request due to its plain text nature aligns with the security protocols expected in 5G communication, as it prevents potential security breaches that could arise from unencrypted messages. Therefore, the UE's action to reject the non-compliant authentication request was in accordance with 5G security standards, demonstrating a secure response to an insecure situation. Secure</p>
143	143	<p>This is 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:</p> <p>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</p> <p>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, UplinkNAS transport, Deregistration request (UE originating) 0.5048840045928955 AMF to UE SACK (Ack=7, Arwnd=106334) , DownlinkNASTransport, Deregistration request (UE terminated) (Junkdown)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 necessary 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 downlink NAS message with a "deregistration request," 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 this deregistration request. The lack of response from the UE could be interpreted in different ways: it might suggest that the UE did not recognize or accept the deregistration request, or it could indicate a failure in processing the message. According to the 3GPP standards, the UE should respond to such requests to maintain a secure and synchronized state with the network. The absence of a response from the UE could potentially leave it in an insecure state, as it may not be properly deregistered from the network, leading to vulnerabilities. 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</p>

144	144	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, which was followed by the AMF sending a "configuration update command" back to the UE. This downlink message from the AMF was protected, as indicated by the security header being both integrity protected and ciphered. The UE responded with a "configuration update complete" message, indicating that it successfully processed the command. The packet capture confirms that the messages were exchanged in a secure manner, with the initial uplink message from the UE and the subsequent downlink message from the AMF both being part of a protected communication session. According to the 3GPP standards, the completion of the 5G-AKA process ensures that subsequent NAS messages are encrypted and integrity protected, which is crucial for maintaining the confidentiality and integrity of the communication. Given that the UE adhered to these security protocols by responding appropriately to the protected configuration update command, the actions taken by the UE can be considered secure. Therefore, based on the interaction and adherence to the 3GPP standards, the UE's communication was secure. Secure</p>
145	145_F	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. Subsequently, the AMF sent a "security mode command" back to the UE, which was protected, as indicated by the security header stating "Integrity protected with new security context (3)." The UE's response to this command was another "security mode complete" message. The use of the 5G-EA0 (null) cipher algorithm suggests that no encryption was applied to the data, but the integrity was protected using the 128-5G-IA2 algorithm. According to the 3GPP standards, while the integrity protection is crucial, the lack of encryption (using a null cipher) could expose the communication to potential eavesdropping, as the data is not encrypted. Therefore, although the integrity of the messages was maintained, the absence of encryption makes the communication insecure against confidentiality threats. Based on this analysis, the action taken by the UE was "Insecure."</p>

146	146	<p>This is 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:</p> <p>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</p> <p>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 message. 0.16037797927856445 AMF to UE SACK (Ack=3, Arwnd=106496) , DownlinkNASTransport, Deregistration accept (UE terminated)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 message, "security mode complete," indicating that it had accepted the security parameters set by the network. However, the subsequent downlink message from the AMF was a "deregistration accept," which was sent as a protected message. The UE did not respond to this message. The packet capture shows that the UE sent a "security mode complete" message, followed by a "registration request," but the AMF responded with a "deregistration accept," effectively terminating the session. According to the 3GPP standards, the UE should have responded to the deregistration message to confirm the termination of the session. The lack of response from the UE could indicate a failure to properly handle the deregistration process, which is a critical aspect of maintaining secure communication. The UE's failure to respond to the deregistration accept message suggests a potential security vulnerability, as it did not follow the expected protocol for session termination. Therefore, based on the 3GPP standards, the action taken by the UE can be considered insecure. Insecure</p>
147	147	<p>This is 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:</p> <p>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)</p> <p>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 message. 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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, establishing a secure context for subsequent communications. The UE then sent a "security mode complete" message to the AMF, indicating that it had successfully configured the security settings. Following this, the AMF sent a "configuration update command" to the UE, which was integrity protected with a new security context, as indicated by the security header. 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 security measure to prevent processing potentially malicious or erroneous messages. According to the 3GPP standards, the UE's response to an unexpected or incompatible message type is a valid security behavior, as it helps maintain the integrity and security of the communication by not processing messages that do not align with the expected protocol state. Therefore, the UE's action in this scenario appears to be secure, as it adhered to the protocol's security measures by flagging an incompatible message type. Secure</p>

148	148	<p>This is 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:</p> <p>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)</p> <p>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) 0.3268871307373047 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In this test scenario, the interaction between the User Equipment (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 environment. 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 actions taken by the UE were secure. Secure</p>
149	149	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, including the ciphering and integrity protection algorithms. However, the AMF subsequently 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. Given that the 5G-AKA was completed and the messages were protected, the UE's actions appear to be secure according to the 3GPP standards. However, the sequence of messages is atypical, and in a real-world scenario, this could indicate a potential issue with the AMF's behavior rather than the UE's security posture. Therefore, based on the information provided and focusing solely on the UE's actions, the UE's communication can be considered "Secure."</p>

150	150	<p>This is 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:</p> <p>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)</p> <p>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) 0.3618440628051758 UE to AMF UplinkNASTransport, Deregistration accept (UE terminated)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 conducted under a secure communication channel established by the 5G-AKA process. This suggests that the UE adhered to the security protocols outlined by the 3GPP, maintaining the integrity and confidentiality of the communication. Therefore, based on the interaction and the security measures in place, the UE's actions can be considered secure. Secure</p>
151	151	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 respond 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 messages are encrypted and protected from potential interception or tampering. Since the identity request was sent in plain text before the completion of 5G-AKA, the UE's lack of response can be considered a secure action. By not responding to an unencrypted identity request, the UE avoids exposing sensitive information, such as the GUTI, which could be intercepted by malicious entities. Therefore, the UE's decision to withhold a response aligns with the security principles outlined by 3GPP, as it prevents the potential compromise of its identity information. Secure</p>

152	152	<p>This is 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:</p> <p>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</p> <p>The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling] 0.0007770061492919922 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Configuration update command</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, followed by the AMF responding 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. 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 to the configuration update command. According to the 3GPP standards, for messages to be securely encrypted, the 5G-AKA procedure must be completed to establish a secure 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 that it did not accept the configuration update command due to the absence of a secure context, which would be a prudent action. However, without further information on the UE's reasoning for not responding, it is difficult to definitively conclude the security posture. Based on the available information, the UE's action of not responding to an unprotected message aligns with maintaining security, but the overall situation remains insecure due to the incomplete 5G-AKA. Therefore, the communication can be considered "Insecure."</p>
153	153	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. Subsequently, 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, specifying the use of the cipher algorithm 128-5G-EA3 and the integrity algorithm 5G-IA0 (null). However, 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 responded with an uplink message indicating a 5GMM status of "Invalid mandatory information." This response suggests that the UE detected an issue with the security mode command, possibly due to the incomplete 5G-AKA process or the use of a null integrity algorithm, which does not provide integrity protection. According to the 3GPP standards, the UE should not proceed with establishing a security context if the integrity protection is not adequately ensured. The UE's action to flag the invalid mandatory information indicates that it did not accept the security mode command under these conditions, which aligns with the security requirements of the 5G standard. Therefore, the UE's response can be considered secure as it adhered to the protocol by not accepting potentially insecure parameters. Secure</p>

154	154	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 this point, which is a prerequisite for establishing a secure communication channel. The UE did not provide any response to the configuration update command from the AMF. According to the 3GPP standards, for messages to be securely encrypted and integrity protected, the 5G-AKA process must be completed to establish the necessary security context. Since the 5G-AKA was not completed, the UE's lack of response to the AMF's protected message suggests that it did not proceed with processing the message without a secure context. This behavior aligns with the security requirements, as the UE should not accept or process messages that are protected without an established security context. Therefore, the UE's action of not responding to the configuration update command without a completed 5G-AKA process can be considered secure according to the 3GPP standards. Secure</p>
155	155	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 UE did not provide any response to this deregistration accept message. According to the 3GPP standards, for messages to be encrypted and protected, 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 initial registration request from the UE was sent without the security context being established. The lack of response from the UE to the deregistration accept message could indicate that the UE did not recognize or process the message due to the absence of a secure context. Based on the 3GPP standards, the UE's action of sending an initial registration request without completing the 5G-AKA and not responding to a protected deregistration message suggests a lack of adherence to the expected security procedures, rendering the communication insecure. Therefore, the UE's actions in this test scenario were "Insecure."</p>

156	156	<p>This is 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:</p> <p>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)</p> <p>The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request, Registration request [RRCEstablishmentCause=mo-Signalling] 0.000786060552978516 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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. Subsequently, the AMF responded with a security mode command, which was protected but utilized null algorithms for both ciphering (5G-EA0) and integrity (5G-IA0). The security header indicated that the message was integrity protected with a new security context. However, the UE responded with a security mode reject, citing an unspecified reason. According to the 3GPP 5G standards, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed before secure communication can occur, ensuring that messages are encrypted and integrity protected. In this scenario, the 5G-AKA was not completed, and the AMF's use of null algorithms for both ciphering and integrity protection means that the communication was not secure. The UE's decision to reject the security mode command is consistent with the 5G standards, as it prevents the establishment of a security context that lacks proper encryption and integrity protection. Therefore, the UE's action to reject the security mode command was appropriate and aligned with maintaining security standards. Secure.</p>
157	157	<p>This is 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:</p> <p>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</p> <p>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 response)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 deregistration request was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered. Despite this, the UE did not provide any response to the deregistration request. According to the 3GPP standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed first, which was not the case here. The lack of a response from the UE could be interpreted as a security measure, as the UE might have detected that the 5G-AKA was not completed and thus chose not to engage further with potentially insecure communication. This behavior aligns with the security protocols outlined by 3GPP, which emphasize the importance of completing authentication procedures before engaging in protected communication. Therefore, the UE's action of not responding to the deregistration request, given the incomplete 5G-AKA, can be considered a secure response to maintain the integrity and confidentiality of its communication. Secure</p>



158	158	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 remained unencrypted. The UE's lack of response to the identity request can be seen as a cautious action, as responding to an unencrypted request could expose sensitive information. By not responding, the UE avoids the risk of transmitting its IMEISV in plain text, which could be intercepted by unauthorized parties. This behavior aligns with security best practices, as it prevents potential exposure of sensitive information when encryption is not in place. Therefore, the UE's action in this scenario can be considered secure. Secure</p>
159	159	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 GMM status message back to the UE, indicating "Roaming not allowed in this tracking area," with a 5GMM Cause value of 13. Notably, this downlink message 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 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 address the security implications of receiving an unencrypted message. Based on the 3GPP standards, the UE's action in this scenario is considered insecure, as it did not ensure the confidentiality and integrity of the communication before proceeding with the exchange of sensitive information. Insecure</p>

160	160	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 configuration update command. Notably, the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed at the time of this interaction. 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)." The UE did not provide a response to this command. According to the 3GPP standards, for NAS messages to be encrypted, the 5G-AKA procedure must be completed to establish security keys. Since the 5G-AKA was not completed, the communication remained unencrypted, which is a security risk. The UE's lack of response to the plain configuration update command could be interpreted as a cautious action, potentially avoiding processing an unencrypted message. However, the fact that the communication was not encrypted due to the incomplete 5G-AKA process indicates a vulnerability in the security of the interaction. Therefore, based on the 3GPP standards, the action taken by the UE in this context is considered insecure. Insecure</p>
161	161	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 was not completed, which is crucial for establishing a secure communication channel. The packet capture indicates that the downlink message from the AMF was sent as "Protected," but without the completion of the 5G-AKA, the messages between the UE and AMF cannot be encrypted as per the 3GPP standards. The UE did not provide any response to the deregistration accept message, which could imply that it did not process the message further. According to the 3GPP standards, the 5G-AKA procedure must be completed to ensure that the communication is secure and encrypted. Since the 5G-AKA was not completed, the UE's communication with the AMF was not secure, as it did not adhere to the necessary security protocols outlined by the 3GPP for encrypted communication. Therefore, the action taken by the UE in this scenario was insecure. Insecure</p>

162	162	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 service accept message. The packet capture indicates that the service accept message from the AMF was sent as a protected message, despite the 5G Authentication and Key Agreement (5G-AKA) procedure not being completed. According to the 3GPP standards, for messages to be encrypted and protected, the 5G-AKA procedure must be completed to establish a secure context. Since the 5G-AKA was not completed, the UE should not have accepted or processed the service accept message as protected, because the necessary security context for encryption and integrity protection was not established. The UE's lack of response to the protected service accept message suggests that it did not process the message, which aligns with the expected behavior when the security context is not established. Therefore, based on the 3GPP standards, the UE's action of not responding to the protected message without a completed 5G-AKA indicates that it adhered to the security protocols. Secure</p>
163	163	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 from the AMF 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 and integrity protected, the 5G-AKA procedure 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. Consequently, the UE's lack of response to the deregistration request could be seen as a failure to engage in a potentially insecure communication, as the security context was not properly set up. This indicates that the UE did not proceed with an action that could compromise its security, adhering to the principle of not responding to messages when the security context is not established. Therefore, based on the 3GPP standards, the UE's action in this scenario can be considered secure. Secure</p>

164	164	<p>This is a security test for a 5G standalone User Equipment (UE). During the NAS communication, after completing the preceding NAS steps, the UE sent an identity response and then The AMF sent security mode command to the UE. The test summary as follows:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 UE sent an identity response, the AMF responded with a security mode command, which was protected and included specific security algorithms: 5G-EA4 for ciphering and 128-5G-IA1 for integrity protection. The security header indicated that the message was integrity protected with a new security context. However, the UE responded with a security mode reject, citing an unspecified reason. 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 UE's rejection of the security mode command could be seen as a precautionary measure to avoid engaging in a potentially insecure communication session. The UE's action to reject the security mode command without a completed 5G-AKA suggests that it adhered to the security protocols by not accepting a security context that might not be fully secure. Therefore, the UE's action was in line with maintaining security as per the 5G standards. Secure</p>
-----	-----	--	--

165	165	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, followed by the AMF issuing a security mode command. Notably, the security mode command was sent as a plain NAS message, indicating that encryption had not yet been established. This is because the 5G Authentication and Key Agreement (5G-AKA) process, which is essential for securing communications, had not been completed. The UE then sent a deregistration request, which was also unencrypted due to the absence of a security context. According to the 3GPP standards, for messages to be secure, the 5G-AKA process must be completed to establish encryption and integrity protection. Since the security mode command was sent in plain text and the UE responded with a deregistration request without an established security context, the communication was not secure. The lack of encryption and integrity protection exposes the communication to potential interception and tampering. Therefore, based on the 3GPP standards, the actions taken by the UE in this scenario were insecure. Insecure</p>
166	166	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 encryption requires the completion of the 5G-AKA process. The UE did not provide any response to the configuration update command. According to the 3GPP standards, for messages to be securely encrypted, the 5G-AKA process must be completed to establish the necessary security keys. Since the 5G-AKA was not completed, the communication was not encrypted, leaving the interaction potentially vulnerable to interception or tampering. The lack of a response from the UE to the configuration update command could indicate a security measure to avoid processing unencrypted or improperly secured messages. Based on this interaction, the UE's action of not responding to the configuration update command without completed 5G-AKA and encryption aligns with secure practices as per 3GPP standards, as it avoids processing potentially insecure messages. Therefore, the action taken by the UE was "Secure."</p>

167	167	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 5G, 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 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 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 equipment information. Therefore, the UE's action of not responding to the plain text identity request can be considered a secure response in this context. Secure</p>
168	168	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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-AKA (Authentication and Key Agreement) procedure. However, the 5G-AKA process 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 initiated a disconnection from the network. According to the 3GPP standards, for messages to be encrypted and secure, the 5G-AKA procedure must be fully completed to establish a secure context. Since the 5G-AKA was not completed, the UE's actions, particularly the sending of the deregistration request, were not protected by the full security context that would typically be established by a completed 5G-AKA. This lack of a complete security context could expose the UE to potential security vulnerabilities, as the communication may not be fully encrypted or authenticated. Therefore, based on the 3GPP standards, the UE's communication in this scenario is considered insecure. Insecure</p>

169	169	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, indicating a cause value 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. 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 remained unencrypted, leaving it vulnerable to interception and potential tampering. The UE's lack of response to the plain text GMM status message suggests that it did not proceed with any further actions, which could be interpreted as a cautious approach. However, the fact that the communication was not encrypted due to the incomplete 5G-AKA process indicates a security lapse. Therefore, based on the 3GPP standards, the UE's communication in this scenario was insecure. Insecure</p>
170	170	<p>This is 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:</p> <p>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</p> <p>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) (5G-AKA process must be completed to establish the necessary security context)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, the UE did not provide any response to the deregistration request. 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 was not fully established, which means the UE's lack of response to the deregistration request could be seen as a failure to handle the situation securely. The UE should ideally have mechanisms to handle unexpected or premature deregistration requests, especially when the security context is not fully established. Therefore, based on the 3GPP standards and the observed behavior, the action taken by the UE was insecure. Insecure</p>

171	171	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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), the UE sent a "security mode complete" message to the AMF, indicating that the security context was established and the UE 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 context is established, all subsequent NAS messages should be encrypted to protect the confidentiality and integrity 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-conscious action, as responding to an unencrypted request could expose sensitive information. Therefore, the UE's decision not to respond to the plain text request aligns with maintaining security standards. In this context, the UE's action was secure. Secure</p>
172	172	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 completed the security mode command, which is a step to ensure that subsequent NAS messages are encrypted and integrity protected. However, the AMF then sent an "identity request" message to the UE 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 security mode is complete, all NAS messages should be encrypted to protect the confidentiality and integrity 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, as responding to an unencrypted request could expose sensitive information. Therefore, the UE's action of not responding to the plain text request aligns with maintaining security as per the 3GPP standards. Secure</p>



173	173	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 essential 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 communications. 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 was completed, and messages should typically be encrypted thereafter. In response to the service rejection, the UE sent a deregistration request to the AMF, indicating its intent to disconnect from the network. The UE's actions appear to be in line with the 3GPP standards, as it attempted to establish a secure communication channel and appropriately responded to the service rejection by deregistering. However, the fact that the AMF's service reject message was sent in plain text raises concerns about the security of the communication. Despite this, the UE's response to deregister upon receiving an unexpected plain text message suggests that it acted prudently to protect itself from potential security threats. Therefore, based on the UE's actions and adherence to the 3GPP standards, the communication can be considered "Secure."</p>
174	174	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 a "security mode complete" message, indicating that it was ready to proceed with secure communications. However, the subsequent message from the AMF was an "authentication request" sent in plain text, which is unusual because, after the completion of 5G-AKA, messages should be encrypted to ensure confidentiality and integrity. The UE did not respond to this plain-text authentication request, which suggests that it adhered to the security protocols by not engaging in potentially insecure communication. According to the 3GPP standards, once the security context is established, all NAS messages should be encrypted. The UE's lack of response to an unencrypted message aligns with these security standards, as it avoided processing a message that could compromise security. Therefore, the UE's actions in this scenario were consistent with maintaining secure communication as per the 5G standard. Secure</p>

175	175	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In the test scenario, the User Equipment (UE) and the Access and Mobility Management Function (AMF) engaged in a sequence of NAS (Non-Access Stratum) communications. After completing 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 proposed by the AMF, which should include encryption and integrity protection for subsequent messages. However, the AMF's subsequent "service accept" message was sent in plain text, which suggests that the message was not encrypted. The UE did not respond to this plain text message, which could imply that it did not accept or process the message due to its lack of encryption. According to the 3GPP standards, once the security mode is complete, all NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the UE did not respond to an unencrypted message aligns with secure behavior, as it suggests the UE is adhering to the requirement for encrypted communication post-security mode completion. Therefore, based on the interaction and the UE's lack of response to an unencrypted message, the UE's actions can be considered secure according to the 5G standard. Secure</p>
176	176	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 the requested identity was the Subscription Concealed Identifier (SUCI). 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. However, 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 potentially compromising its security by transmitting the SUCI 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</p>

177	177	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 a critical point of concern. 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 confidentiality and integrity. The fact that the AMF sent the authentication request in plain text suggests a deviation from the expected secure communication protocol. Furthermore, the UE did not respond to the authentication request, which could indicate a failure to recognize or process the message due to its insecure nature. This lack of response might be a security measure by the UE to avoid engaging in potentially compromised communication. However, the initial acceptance of a plain text message from the AMF could still expose the UE to security risks. Based on the 3GPP standards, the UE's action of not responding to an unencrypted authentication request aligns with secure practices, but the acceptance of the plain text message itself is concerning. Therefore, the overall interaction is deemed insecure due to the initial acceptance of an unencrypted message. Insecure</p>
178	178	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 an "identity request" message to the UE, requesting the Subscription Concealed Identifier (SUCI). Notably, this identity request was sent in plain text, which is a critical point of concern. In response, the UE sent a "deregistration request (UE originating)" message. According to the 3GPP standards, after the 5G Authentication and Key Agreement (5G-AKA) is completed, 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 suggests a potential vulnerability, as sensitive information like the SUCI should not be exposed in an unencrypted format. The UE's decision to send a deregistration request instead of responding with the requested SUCI could be interpreted as a protective measure to avoid transmitting sensitive information over an insecure channel. This action aligns with security best practices, as it prevents the potential exposure of the subscriber's identity. Therefore, based on the UE's response to the plain text identity request, the action taken by the UE can be considered secure, as it prioritized the protection of sensitive information. Secure</p>

179	179	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 completed. Following this, the AMF sent a "configuration update command" to the UE. Notably, this downlink message from the AMF was sent as a plain NAS message, meaning it was not encrypted. Subsequently, the UE sent a "deregistration request" originating from the UE itself. According to the 3GPP standards, once the 5G Authentication and Key Agreement (5G-AKA) is completed, all NAS messages should be encrypted to ensure secure communication. However, in this test, the configuration update command was sent in plain text, which is a deviation from the expected secure communication protocol. The UE's response to this unencrypted message was to send a deregistration request, which could be interpreted as a security measure to terminate the session due to the receipt of an unencrypted message. This action suggests that the UE recognized the potential security risk and acted to mitigate it. Therefore, based on the UE's response to the unencrypted message, the action taken by the UE can be considered secure as it aligns with the security principles of terminating communication upon detecting a security anomaly. Secure</p>
180	180	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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)". Subsequently, the UE sent a deregistration request, which was UE-originating. According to the 3GPP standards, once the 5G-AKA process is completed, NAS messages should be encrypted to ensure confidentiality and integrity. However, in this test, the AMF sent a plain configuration update command, which suggests that the message was not encrypted. This lack of encryption could potentially expose sensitive information to interception or manipulation, indicating a security vulnerability. The UE's action of sending a deregistration request following the receipt of a plain message could be interpreted as a response to an insecure communication environment. Based on the 3GPP standards, the communication in this scenario is considered insecure due to the transmission of unencrypted messages after the completion of the 5G-AKA process. Insecure</p>

181	181	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 5G Authentication and Key Agreement (5G-AKA) procedure is completed. The 5G-AKA was marked as completed, yet the AMF's authentication request was not encrypted, indicating a potential security lapse. The UE did not respond to the authentication request, which could suggest that it detected the anomaly of receiving a plain text message when it should have been encrypted. This lack of response could be interpreted as a security measure by the UE to avoid engaging in potentially insecure communication. Based on the 3GPP standards, the UE's action of not responding to an unencrypted authentication request after the 5G-AKA completion aligns with secure communication practices, as it avoids potential exposure of sensitive information. Therefore, the UE's action in this scenario can be considered "Secure."</p>
-----	-----	--	---

182	182	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 value 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 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. 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. However, the initial sending of the uplink NAS transport message without ensuring the encryption status of subsequent messages could be seen as a vulnerability. Overall, while the UE's non-response to the plain text message might suggest a cautious approach, the initial interaction does not fully align with the secure communication practices expected in 5G standards. Therefore, the UE's actions in this scenario can be considered "Insecure."</p>
-----	-----	--	--

183	183	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In this test scenario, the interaction between the User Equipment (UE) and the Access and Mobility Management Function (AMF) begins with the UE sending 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 because, according to the 5G standard outlined by 3GPP, messages should be encrypted after the 5G Authentication and Key Agreement (5G-AKA) procedure is completed. The 5G-AKA procedure is indicated as completed in the test summary, suggesting that subsequent messages should be encrypted to ensure confidentiality and integrity. However, the AMF's authentication request was sent in plain text, which could expose sensitive information to potential interception. The UE's response to this situation was to send a deregistration request, which could be interpreted as a security measure to terminate the session due to the detection of an insecure communication attempt. This action aligns with the security principles of the 5G standard, which prioritize the protection of user data and the integrity of the communication process. Therefore, the UE's decision to deregister in response to receiving an unencrypted authentication request can be considered a secure action, as it prevents further communication that could compromise security. Secure.</p>
-----	-----	--	---

184	184	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 International Mobile Equipment Identity (IMEI) in plain text. Instead of responding with the requested identity, the UE sent a deregistration request, indicating a UE-originated deregistration. This sequence of actions suggests that the UE did not comply with the identity request from the AMF. According to the 3GPP standards, once the 5G-AKA is completed, NAS messages should be encrypted to ensure confidentiality and integrity. The AMF's identity request was sent in plain text, which could be considered a security risk, as sensitive information like the IMEI should be protected. The UE's decision to send a deregistration request instead of providing the IMEI could be interpreted as a security measure to avoid transmitting sensitive information in an unprotected manner. This behavior aligns with the security principles of minimizing exposure of sensitive data. Therefore, based on the 3GPP standards and the UE's response to the plain text identity request, the UE's action can be considered secure. Secure</p>
185	185	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, indicating that no network slices were available, with a 5GMM Cause value of 62. Notably, this downlink message was sent in plain text, which is a critical point of concern. 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 a plain text message suggests a potential vulnerability, but since the focus is on the UE's actions, it is important to note that the UE did not respond to the registration reject message. This lack of response could be interpreted as the UE not taking any further action that might compromise security. However, the absence of encryption in the downlink message from the AMF is a deviation from the expected secure communication protocol. Given that the UE did not engage in any further communication after receiving the plain text message, it did not actively compromise security, but the situation highlights a potential risk area in the communication process. Therefore, while the UE's actions were not directly insecure, the overall interaction raises concerns about adherence to security standards. Insecure.</p>



186	186	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 in plain text, as indicated by the security header being a plain NAS message (0). The UE, instead of responding to the security mode command, sent a deregistration request, which suggests that the UE did not proceed with the security mode command process. According to the 3GPP standards, after the 5G-AKA is completed, the NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent a plain text security mode command and the UE did not respond to it, opting instead to deregister, indicates a potential security issue. The UE's action of not responding to an unencrypted security mode command could be seen as a protective measure against a potential security threat, as it avoids proceeding with a potentially insecure communication. However, the lack of response also means that the security procedures were not completed as expected. Therefore, while the UE's action might be cautious, it does not align with the expected secure communication process as per the 5G standard. In conclusion, the UE's action in this scenario is "Insecure."</p>
187	187	<p>This is 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:</p> <p>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</p> <p>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 2.197467088699341 AMF to UE SACK (Ack=11, Arwnd=106334) , DownlinkNASTransport, Configuration update command 2.197576045989902 AMF to UE DownlinkNASTransport, Identity request</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, specifically requesting the International Mobile Equipment Identity Software Version (IMEISV) 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, subsequent NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. 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 identity information over an unencrypted channel. By not responding to the plain text identity request, the UE adhered to the security principles of the 5G standard, which prioritize the protection of user identity and data. Therefore, the UE's action in this scenario was secure, as it prevented the potential exposure of sensitive information due to the lack of encryption in the AMF's request. Secure</p>

188	188	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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, meaning 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 message could be interpreted as a failure to recognize or react to this security breach. Therefore, based on the 3GPP standards, the UE's action in this scenario was insecure, as it did not ensure the confidentiality and integrity of the communication.</p> <p>Insecure</p>
189	189	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In the security test for the 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) procedure was completed prior to this exchange, which is a prerequisite for establishing secure communication. However, the security mode command from the AMF was sent as a plain NAS message, indicated by the security header value of 0, meaning it was not encrypted. According to the 3GPP standards, after the 5G-AKA procedure, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. The UE did not respond to the plain security mode command, which suggests that it did not proceed with an insecure communication setup. This behavior aligns with the 3GPP standards, as the UE should not accept or respond to unprotected messages when encryption is expected. Therefore, the UE's action of not responding to the plain message can be considered secure, as it adhered to the security protocols by not engaging in potentially insecure communication.</p> <p>Secure</p>

190	190	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 request. The 5G-AKA procedure was completed, which is a prerequisite for establishing a secure communication channel. However, the AMF sent the authentication request message in plain text, which is unusual since, after the completion of 5G-AKA, messages should be encrypted to ensure confidentiality and integrity. The UE did not respond to the authentication request, which could indicate that it detected the message was not encrypted and thus potentially insecure. According to the 3GPP standards, after the 5G-AKA procedure, the UE should expect encrypted messages, and any deviation from this could be a security risk. The UE's lack of response suggests it adhered to the security protocols by not engaging with an unencrypted message, which aligns with the expected behavior to prevent potential security breaches. Therefore, based on the UE's actions and adherence to the 3GPP standards, the UE's response can be considered secure.</p> <p>Secure</p>
-----	-----	---	---

191	191_F	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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-AKA (Authentication and Key Agreement) procedure, the UE sent a service request to the AMF. In response, the AMF sent an authentication request back to the UE. Notably, this downlink message from the AMF was sent in plain text, which is unusual as messages should be encrypted post-authentication. The authentication request included parameters such as ABBA, RAND, AUTN, and ngKSI values. The UE responded with an authentication failure message, indicating that the ngKSI (NAS key set identifier) was already in use, suggesting that the UE detected a potential security issue with the reuse of an existing security context. According to the 3GPP standards, the UE's response is appropriate and secure, as it is designed to prevent replay attacks and ensure that each authentication session is unique. By rejecting the authentication request due to the reuse of an ngKSI, the UE is adhering to the security protocols outlined by 3GPP, which aim to protect against unauthorized access and ensure the integrity of the communication. Therefore, the action taken by the UE was secure. Secure</p>
192	192	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 securing NAS messages. However, the identity request from the AMF was sent in plain text, which is unusual given that encryption should be applied after the successful completion of 5G-AKA. The AMF requested the Temporary Mobile Subscriber Identity (TMSI) from the UE, but the UE did not respond. According to the 3GPP standards, after the 5G-AKA procedure, NAS messages should be encrypted to protect the subscriber's identity and other sensitive information. The UE's lack of response to an unencrypted identity request suggests that it adhered to security protocols by not transmitting sensitive information over an insecure channel. This behavior aligns with the 3GPP standards, which emphasize the importance of protecting user identity and data integrity. Therefore, the UE's action of not responding to the plain text identity request can be considered a secure response to maintain the confidentiality and integrity of the communication. Secure</p>

193	193	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, NAS messages should be encrypted and integrity protected to ensure confidentiality and authenticity. The lack of a response from the UE could suggest that it did not recognize the security header or that there was an issue with the message's integrity or encryption, which could indicate a potential security vulnerability. The UE's failure to respond to a protected message, especially when the security header is unknown, raises concerns about its ability to handle secure communications as per the 5G standard. Therefore, based on the observed behavior and the standards outlined by 3GPP, the action taken by the UE appears to be insecure. Insecure</p>
194	194	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 maintaining secure communication channels. 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</p>

195	195_F	<p>This is 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:</p> <p>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</p> <p>The packet capture during the test using wireshark is: 9.68098980697632 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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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), which is crucial for establishing a secure communication channel, the UE sent a service request to the AMF. In response, the AMF issued an identity request to the UE, specifically requesting the Subscription Concealed Identifier (SUCI). Notably, the identity request from the AMF 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 procedure is completed, subsequent NAS messages should be encrypted to ensure confidentiality and integrity. However, in this test, the AMF's identity request 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 with an identity response, without ensuring the message was encrypted, suggests a lapse in adhering to the security protocols expected post-5G-AKA. Therefore, based on the 3GPP standards, the UE's action in this scenario can be considered insecure, as it did not ensure the confidentiality of the identity information being transmitted. Insecure</p>
196	196	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 to the configuration update command. According to the 3GPP standards, after the 5G-AKA procedure, NAS messages should be encrypted and integrity protected to ensure secure communication. The lack of a 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 absence of a response raises concerns about the UE's ability to handle protected messages correctly, which is critical for maintaining secure communication. 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</p>

197	197	<p>This is 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:</p> <p>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</p> <p>The packet capture during the test using wireshark is: 0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=no-Signalling] 0.0005860328674316406 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated communication)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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) process 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 properly interpret or respond to the deregistration request. Consequently, the UE provided no response to the AMF's deregistration request. This lack of response suggests that the UE did not engage in potentially insecure communication without the proper security context established by the 5G-AKA process. Therefore, based on the 3GPP standards, the UE's action of not responding to the deregistration request without a completed 5G-AKA process can be considered secure, as it avoided engaging in communication that could have been insecure. Secure</p>
198	198	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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 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 request aligns with maintaining security as per the 3GPP standards, as it avoids transmitting sensitive information over an unprotected channel. Secure</p>

199	199	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 had successfully established a secure communication context. 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 context is established, all NAS messages should be encrypted to protect the confidentiality and integrity 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 unprotected manner. This behavior aligns with the 3GPP standards, which emphasize the importance of maintaining encryption for all subsequent NAS messages after security mode completion. Therefore, the UE's action of not responding to an unencrypted identity request is considered secure according to the 5G standard. Secure</p>
200	200	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 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-conscious action, as responding could have compromised the SUCI. By not responding, the UE adhered to the security principles of the 5G standard, which prioritize encrypted communication to protect user identity and data. Therefore, the UE's action in this scenario was secure. Secure</p>



201	201	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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), the UE sent a "security mode complete" message to the AMF, indicating that the security mode command was successfully processed. Subsequently, the AMF sent an "identity request" message to the UE, requesting the International Mobile Equipment Identity (IMEI) of 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 is completed, all subsequent NAS messages should be encrypted to ensure confidentiality and integrity. However, the AMF's identity request was sent unencrypted, which could expose sensitive information if intercepted. The UE did not respond to this request, which could be interpreted as a security measure to avoid transmitting sensitive information over an unencrypted channel. This lack of response aligns with secure communication practices, as it prevents the potential exposure of the UE's IMEI. Therefore, based on the 3GPP standards and the actions taken by the UE, the UE's decision not to respond to an unencrypted identity request can be considered a secure action. Secure</p>
202	202	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 the security context was established and the UE was ready for 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 security context is established, all NAS messages should be encrypted to protect the integrity and confidentiality of the communication. The AMF's decision to send 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-conscious action, 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 the 3GPP security standards, as it avoids potential exposure of sensitive information. Secure.</p>

203	203	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 channel with the AMF. 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 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 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 request aligns with maintaining security as per the 3GPP standards. Secure</p>
204	204	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 the security mode command was successfully processed and 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 Software Version (IMEISV) 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 after the security mode was established 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. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security as per the 3GPP standards. Secure</p>

205	205	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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, which is unusual given that encryption should be in place after 5G-AKA completion. The AMF requested the Subscription Concealed Identifier (SUCI) from the UE, but the UE did not respond. According to the 3GPP standards, after the 5G-AKA procedure, NAS messages should be encrypted to protect sensitive information such as the SUCI. The UE's lack of response to an unencrypted identity request aligns with security best practices, as responding to such a request could expose sensitive information. Therefore, the UE's action of not responding to the plain text identity request is consistent with maintaining security as per the 5G standards. Secure</p>
206	206	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 the requested identity was the Subscription Concealed Identifier (SUCI). 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 confidentiality and integrity. The fact that the AMF sent the identity request in plain text is a deviation from the expected secure communication protocol. However, 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. Therefore, the UE's decision not to respond to the plain text identity request aligns with maintaining security standards by not transmitting potentially sensitive information without encryption. Based on this analysis, the UE's action was secure. Secure</p>

207	207	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 was acknowledged by the AMF. 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 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 the confidentiality and integrity of the communication. However, the AMF's identity request was sent in plain text, which could potentially expose sensitive information if intercepted. The UE did not respond to this plain text request, which aligns with secure behavior as it avoids transmitting sensitive identity information over an unprotected channel. By not responding, the UE effectively mitigated the risk of exposing the SUCI in an insecure manner. Therefore, based on the 3GPP standards and the observed behavior, the UE's action of not responding to the plain text identity request was secure and appropriate under the circumstances. Secure.</p>
208	208	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 and requested the SUCI, which is sensitive information, raises a security concern. 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 in an unprotected manner. This behavior aligns with the 3GPP standards, which emphasize the importance of protecting subscriber identity and ensuring secure communication. Therefore, the UE's action of not responding to the plain text identity request is considered secure as it prevents potential exposure of sensitive information. Secure</p>

209	209	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. The AMF requested the Subscription Concealed Identifier (SUCI) from the UE, but the UE did not respond. 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 the identity request in plain text suggests a potential vulnerability, as sensitive information like the SUCI should not be transmitted unencrypted. 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 decision not to respond to the unencrypted identity request aligns with the security principles outlined by 3GPP, as it avoids the risk of exposing the SUCI in an insecure manner. Based on this analysis, the UE's action was secure. Secure</p>
210	210	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 and requested the SUCI, which is sensitive information, raises a security concern. 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 in an unprotected manner. This behavior aligns with the 3GPP standards, which emphasize the importance of protecting subscriber identity and ensuring secure communication. Therefore, the UE's action of not responding to the plain text identity request is considered secure as it prevents potential exposure of sensitive information. Secure</p>

211	211	<p>This is 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:</p> <p>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</p> <p>The packet capture during the test using wireshark is: 4.666033029556274 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originated) 4.666288137435913 AMF to UE SACK (Ack=20, Arwnd=106429) , DownlinkNASTransport, Identity request</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 "registration complete" message to the AMF, indicating that the initial registration process was finalized. 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 unusual given that the 5G-AKA process should have established a secure communication channel, encrypting subsequent messages. The UE, however, did not respond to this identity request. According to the 3GPP standards, after the 5G-AKA procedure, all NAS messages should be encrypted to protect the subscriber's identity and other sensitive information. The UE's lack of response to an unencrypted identity request suggests that it adhered to security protocols by not transmitting sensitive information over an insecure channel. This behavior aligns with the 3GPP standards, which emphasize the importance of maintaining confidentiality and integrity of the communication. Therefore, the UE's action in this scenario can be considered secure. Secure</p>
212	212	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. Following this, the AMF sent an identity request to the UE, requesting the International Mobile Equipment Identity Software Version (IMEISV). Notably, the identity request was sent in plain text, which is a critical point of concern. 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 identity request was sent unencrypted, and the UE did not respond to this request. The UE's lack of response can be interpreted as a security measure, as responding to an unencrypted identity request could expose sensitive information. By not responding, the UE potentially avoided a security breach, adhering to the principle of not transmitting sensitive information over an insecure channel. Therefore, based on the 3GPP standards and the UE's actions, the UE's behavior in this scenario can be considered secure. Secure</p>

213	213	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 containing an identity request, which was transmitted in plain text. 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, 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. However, the UE's lack of response to the plain text identity request can be interpreted as a security measure, as it avoided transmitting sensitive information like the SUCI over an unencrypted channel. 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 the plain text identity request can be considered secure, as it prevented potential exposure of sensitive information.</p> <p>Secure</p>
214	214	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 outlined by 3GPP, which emphasize the importance of protecting subscriber identity and other sensitive data. Therefore, the UE's action of not responding to an unencrypted identity request can be considered secure, as it prevents the exposure of the TMSI in an insecure manner.</p> <p>Secure</p>

215	215	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 an identity request message to the UE, requesting the International Mobile Equipment Identity (IMEISV). Notably, this identity request was sent in plain text, which is a critical point of concern. According to the 3GPP standards, after the successful completion of 5G-AKA, NAS messages should be encrypted to protect sensitive information such as the IMEISV. The UE, however, did not respond to the identity request. This lack of response could be interpreted as a security measure by the UE to avoid transmitting sensitive information over an unencrypted channel. Given that the UE refrained from sending its IMEISV in response to an unencrypted request, it adhered to the security principles of protecting sensitive information, as outlined by the 3GPP standards. Therefore, the UE's action in this scenario can be considered secure. Secure</p>
216	216	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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, 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 action of not responding to the plain text identity request aligns with the security principles outlined by 3GPP, as it avoids the risk of exposing sensitive information in an unprotected manner. Secure</p>



217	217	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 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 plain (unencrypted) identity request message to the UE, requesting the International Mobile Equipment Identity Software Version (IMEISV). The UE, however, did not provide a response to this request. According to the 3GPP standards, after the successful completion of 5G-AKA, NAS messages should be encrypted to protect sensitive information such as the IMEISV. The AMF's decision to send the identity request in plain text could expose the UE to potential security risks, as it involves the transmission of sensitive information without encryption. The UE's lack of response to the unencrypted identity request can be interpreted as a security-conscious action, as it avoids transmitting sensitive information over an insecure channel. This behavior aligns with 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 is considered secure. Secure</p>
218	218	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 to the AMF. 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 a critical point of analysis. According to the 3GPP standards, once the 5G-AKA procedure is completed, NAS messages should be encrypted to ensure the confidentiality and integrity of the communication. However, the AMF's identity request was sent unencrypted, which could expose sensitive information if intercepted. The UE did not respond to this request, which could be interpreted as a security measure to avoid transmitting sensitive information over an unencrypted channel. This lack of response from the UE aligns with the security principles of the 5G standard, as it prevents potential exposure of the TMSI in an insecure manner. Therefore, the UE's action of not responding to an unencrypted identity request can be considered a secure practice in this context. Secure</p>

219	219	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. In response, the AMF sent a downlink NAS transport message containing 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</p>
220	220	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 downlink identity request message. Notably, 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, 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. The UE's lack of response to the plain text identity request can be interpreted as a security-conscious action, as it avoids transmitting potentially sensitive information without encryption. This behavior aligns with the security principles outlined by 3GPP, which emphasize the importance of protecting subscriber identity and other sensitive data. Therefore, the UE's decision not to respond to the unencrypted identity request can be considered a secure action in this context. Secure</p>

221	221	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 packet capture indicates that the downlink message from the AMF, specifically the service accept message, was sent in plain text. This suggests that the message was not encrypted, which is contrary to the expectation that, after the successful completion of 5G-AKA, all NAS messages should be encrypted to maintain confidentiality and integrity as per the 3GPP standards. The UE's lack of response to the plain text message could imply a failure to recognize or react to the security lapse, which raises concerns about its adherence to security protocols. Given that the UE did not respond to the unencrypted message, it suggests a potential vulnerability in its security handling. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario appears to be insecure. Insecure</p>
222	222	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 test results indicate that the downlink message from the AMF, specifically the service accept, 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 UE did not respond to the plain text message from the AMF suggests that it may have detected the lack of encryption and chose not to proceed with the communication, which aligns with secure behavior as per the 3GPP standards. Therefore, the UE's action of not responding to an unencrypted message can be considered secure, as it indicates adherence to the expected security protocols by not engaging in potentially insecure communication. Secure</p>

223	223	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 applied to 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</p>
224	224	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 is a deviation from the expected secure communication protocol. The UE did not provide any response to the service reject message, which could be interpreted as a lack of further action or acknowledgment from the UE. The absence of encryption in the downlink message suggests a potential vulnerability, as it exposes the communication to interception and tampering. Therefore, based on the 3GPP standards and the observed interaction, the UE's communication in this scenario can be considered insecure due to the lack of encryption in the downlink message from the AMF. Insecure</p>

225	225	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 expected in a 5G environment, as it should have either rejected the unencrypted message or taken steps to re-establish a secure communication channel. Therefore, based on the interaction and the 3GPP standards, the action taken by the UE was insecure. Insecure</p>
226	226	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 synchronization failure with a 5GMM Cause value of 21. 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 service reject 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 security measure, as it did not proceed with any further actions that could compromise its security. This behavior aligns with the 3GPP standards, which emphasize the importance of maintaining secure communication channels. Therefore, the UE's action of not responding to an unencrypted message can be considered secure, as it avoided engaging in potentially insecure communication. Secure</p>

227	227	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 included the cipher algorithm 5G-EA6 and the integrity algorithm 128-5G-IA2, both of which are standard algorithms for securing 5G communications. However, the UE did not provide a response to the security mode command, which is a critical step in establishing a secure communication channel. According to the 3GPP standards, the UE should respond to the security mode command to confirm the security algorithms and establish a secure connection. The absence of a response from the UE suggests a failure to complete the security procedure, 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 necessary steps to ensure a secure communication channel.</p> <p>Insecure</p>
-----	-----	---	--

228	228	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 it was encrypted. However, the security mode command used the 5G-EA0 (null) ciphering algorithm and the 5G-IA0 (null) integrity algorithm, both of which are essentially no encryption and no integrity protection, respectively. The security header was marked as unknown, and crucially, the UE did not provide any response to the security mode command. According to the 3GPP standards, after the 5G-AKA procedure, the UE should engage in secure communication by responding to the security mode command with appropriate encryption and integrity protection. The lack of response from the UE suggests a failure to engage in secure communication, as it did not acknowledge or process the security mode command, leaving the communication potentially vulnerable. Therefore, based on the 5G standard outlined by 3GPP, the action taken by the UE was insecure. Insecure</p>
229	229	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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, which is a deviation from the expected behavior as per the 3GPP standards, where messages should be encrypted after the successful completion of 5G-AKA to ensure confidentiality and integrity. The UE did not provide any response to the plain message, which could suggest a lack of proper handling of unencrypted messages or a failure to adhere to security protocols. Based on the 3GPP standards, the UE should have either rejected the plain message or taken steps to ensure secure communication. The lack of response from the UE to an unencrypted message indicates a potential security vulnerability, as it did not enforce the expected security measures. Therefore, the action taken by the UE in this scenario was insecure. Insecure</p>

230	230	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In the security test for the 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" message. Notably, the security mode command was sent as a plain NAS message, which is indicated by the security header being set to "Plain NAS message (0)." This means that the message was not encrypted, even though the 5G-AKA procedure, which is responsible for establishing security keys for encryption and integrity protection, was completed. The cipher and integrity algorithms specified were 5G-EA4 and 5G-IA5, respectively, but these were not applied to the security mode command message. The UE did not respond to this command. According to the 3GPP standards, after the 5G-AKA procedure, all subsequent NAS messages should be encrypted and integrity protected to ensure secure communication. 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 that it detected the insecure nature of the message and chose not to proceed, which would be a secure behavior. However, without further information on the UE's reasoning for not responding, it is difficult to definitively conclude the security posture. Based on the available information, the UE's action of not responding to an unencrypted security mode command aligns with secure practices, as it avoids engaging in potentially insecure communication. Secure</p>
-----	-----	--	--



231	231	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 fact that this command was sent in plain text (indicated by the security header being a plain NAS message) is concerning, as it exposes the message to potential eavesdropping. The UE did not respond to this command, which could indicate a failure to proceed with the security setup. According to the 3GPP standards, the security mode command should be protected to ensure the integrity and confidentiality of the communication. The lack of response from the UE suggests that it did not engage in the necessary security procedures, leaving the communication vulnerable. Therefore, based on the 5G standard outlined by 3GPP, the action taken by the UE was insecure, as it did not establish a secure communication channel following the initial authentication process. Insecure</p>
232	232	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, indicating that it was not 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, upon receiving an unencrypted authentication reject message, did not provide any response. This lack of response from the UE can be interpreted as a security measure, as it did not engage further with a potentially insecure message. The UE's decision to not respond to an unencrypted message aligns with the security principles of the 5G standard, which emphasize the importance of encrypted communication to protect against potential threats. Therefore, the UE's action of not responding to the plain-text message can be considered secure, as it avoided further interaction that could compromise its security. Secure.</p>

233	233	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, the communication between the UE and the network 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 post-authentication. Therefore, the UE's action of not responding to an unencrypted message can be considered a secure response, as it avoids potential security vulnerabilities that could arise from processing or responding to plain text messages. Secure</p>
234	234	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. Notably, the identity request from the AMF was sent in plain text, and the requested identity was the Temporary Mobile Subscriber Identity (TMSI). 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 a potential security risk. 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. Therefore, the UE's decision not to respond to the plain text identity request aligns with maintaining security standards by not transmitting potentially sensitive information without encryption. Based on this analysis, the UE's action was secure in the context of the 5G standard outlined by 3GPP. Secure</p>

235	235	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. Notably, the identity request from the AMF was sent in plain text, and the requested identity was the International Mobile Equipment Identity Software Version (IMEISV). 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 communication was not encrypted, which is a potential security risk. 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. Therefore, the UE's action of not responding to the plain text identity request aligns with maintaining security by not transmitting sensitive information without encryption. Based on this analysis, the UE's action was secure. Secure</p>
236	236	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 and compromise the security of the communication. Therefore, despite the UE's actions being in line with the protocol, the overall communication was insecure due to the plain transmission of the security mode command by the AMF. Insecure</p>

237	237	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 where the AMF instructs the UE on which ciphering and integrity protection algorithms to use for subsequent NAS messages. In this test, the cipher algorithm used was 5G-EA5, and 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 secure communication parameters. The lack of response from the UE suggests a failure to comply with the expected security procedures, potentially leaving the communication unprotected or improperly configured. This behavior is considered insecure as it does not adhere to the 5G security standards that require both encryption and integrity protection to ensure the confidentiality and integrity of the communication. Therefore, the action taken by the UE in this scenario is deemed insecure. Insecure</p>
238	238	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 in an unencrypted format would be insecure. By not responding, the UE avoids exposing potentially sensitive information without the protection of encryption, which aligns with secure communication practices. Therefore, based on the 3GPP standards and the context of the test, the UE's action of not responding to the plain text request can be considered secure. Secure</p>

239	239	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 seen as a cautious action, as responding to an unencrypted request could expose sensitive information. Therefore, the UE's decision not to respond to the plain text identity request aligns with maintaining security standards by avoiding the transmission of sensitive information over an unprotected channel. Based on this analysis, the UE's action was "Secure."</p>
240	240	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, once 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 engage in a secure communication process, as it did not proceed with the expected encrypted communication. This behavior suggests that the UE did not adhere to the security protocols outlined by the 3GPP standards, which require encryption of NAS messages post-authentication. Therefore, based on the interaction and the standards, the action taken by the UE was insecure. Insecure</p>

241	241	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 unexpected after the completion of the security mode procedure. This downlink message was protected, utilizing the cipher algorithm 5G-EA7 and the integrity algorithm 128-5G-IA2, but the security header was marked as unknown. The UE did not respond to this subsequent security mode command from the AMF. According to the 3GPP standards, once the security mode complete message is sent by the UE, the security context should be established, and further security mode commands should not be necessary unless there is a change in security parameters or a re-establishment of the security context. The lack of response from the UE to the unexpected security mode command suggests that the UE adhered to the standard protocol by not engaging in potentially insecure or redundant procedures. Therefore, the UE's action of not responding to the unexpected security mode command can be considered secure, as it aligns with the expected behavior outlined by the 3GPP standards for maintaining a secure communication session. Secure</p>
-----	-----	---	---

242	242	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 standards, after the 5G-AKA process, the UE should respond to the security mode command to establish a secure communication channel using the specified algorithms. The lack of response from the UE suggests a failure to complete the security setup, which is a critical step in ensuring secure communication. This absence of response could indicate a potential vulnerability or misconfiguration in the UE's handling of security procedures. Therefore, based on the 3GPP standards, the UE's action in this scenario appears to be insecure, as it did not complete the necessary steps to secure the communication channel. Insecure</p>
-----	-----	---	---

243	243	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 authentication response to the AMF. Subsequently, the AMF sent a security mode command back to the UE. Notably, this downlink message from the AMF was sent as a plain NAS message, which means it was not encrypted. The UE, however, did not provide any response to this security mode command. 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 message indicates a potential vulnerability, but the focus here is on the UE's actions. The UE's lack of response to an unencrypted security mode command suggests that it did not proceed with potentially insecure communication, which aligns with secure behavior as per the 3GPP standards. By not responding to a plain message, the UE avoided engaging in a potentially insecure exchange. Therefore, based on the UE's actions, the communication can be considered secure. Secure</p>
-----	-----	---	---



244	244	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 establishing a secure communication channel. Following this, the UE sent a "security mode complete" message to the AMF, indicating that it had accepted the security parameters. However, the AMF then sent a "security mode command" back to the UE, which was transmitted as a plain message without encryption. The ciphering algorithm used was 5G-EA0, which is a null algorithm, meaning no encryption was applied, and the integrity algorithm was 128-5G-IA2. The security header indicated a plain NAS message, and the UE did not respond to this command. According to the 3GPP standards, after the 5G-AKA procedure, messages should be encrypted to ensure confidentiality and integrity. The use of a null cipher algorithm and the transmission of a plain message from the AMF suggest a lack of encryption, which is not aligned with the security expectations of the 5G standard. The UE's lack of response to the plain security mode command could indicate a failure to maintain secure communication. Therefore, based on the 3GPP standards, the actions taken by the UE in this scenario appear to be insecure. Insecure</p>
245	245	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 between the UE and the AMF are encrypted. Since the 5G-AKA was not completed, the communication was not encrypted, and the identity request was sent in plain text, which could expose sensitive information if the UE responded. The UE's lack of response to the identity request in plain text suggests a cautious approach, potentially avoiding the exposure of sensitive information. Based on the 3GPP standards, the UE's action of not responding to an unencrypted identity request aligns with secure communication practices, as it prevents the transmission of sensitive information over an insecure channel. Therefore, the UE's action can be considered secure. Secure</p>

246	246	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, under controlled test conditions, 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 been completed, which is a prerequisite for encrypting messages. 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 UE should not respond to identity requests sent in plain text when the 5G-AKA procedure has not been completed, as this could expose sensitive information. The UE's lack of response to the plain text identity request aligns with the security protocols outlined by 3GPP, as it prevents potential exposure of the TMSI in an unencrypted format. Therefore, the UE's action in this scenario was secure, as it adhered to the standard security practices by not responding to an unprotected identity request. Secure</p>
247	247	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, specifically asking for the IMEISV, which was sent in plain text. 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 between the UE and the AMF 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 could be interpreted as a security measure to avoid transmitting 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 an unencrypted state can be considered a secure approach in this context. Secure</p>

248	248	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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) procedure. 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 a secure communication channel, as it sets the encryption and integrity algorithms for subsequent 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 concerning. According to 3GPP standards, the UE should respond to the security mode command to confirm the security algorithms and establish a secure communication channel. 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 a secure communication channel after receiving the security mode command. Insecure</p>
249	249	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 securing NAS messages. However, the configuration update command from the AMF was sent as a plain NAS message, indicated by the security header value of 0, meaning it was not encrypted. The UE did not provide any response to this plain message. 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 message and did not respond suggests a potential security vulnerability, as it did not adhere to the expected behavior of rejecting or ignoring unencrypted messages post-authentication. This lack of response could indicate that the UE is not properly enforcing the security measures required by the 5G standard, which could expose it to security risks. Therefore, based on the interaction and the standards outlined by 3GPP, the action taken by the UE was insecure. Insecure</p>

250	250	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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, 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. Secure</p>
251	251	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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 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 was not encrypted, leaving the identity request vulnerable to security threats. 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 without encryption could expose sensitive information. Therefore, the UE's decision to withhold a response in this context aligns with maintaining security standards by avoiding the transmission of potentially sensitive data over an unprotected channel. In conclusion, the UE's action was "Secure."</p>

252	252	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 transmitting 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 can be considered secure according to the 5G standard outlined by 3GPP. Secure</p>
253	253	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, and it specifically requested the Globally Unique Temporary Identifier (GUTI) from the UE. However, the UE did not provide any response to this request. According to the 3GPP standards, after the completion of the 5G Authentication and Key Agreement (5G-AKA), all 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 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 potentially sensitive information without encryption. This behavior aligns with the security principles outlined by 3GPP, which emphasize the importance of protecting user identity and data. Therefore, the UE's decision not to respond to an unencrypted identity request can be considered a secure action in this context. Secure</p>

254	254	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 packet capture indicates that the downlink message from the AMF was sent in plain text, which suggests that encryption was not applied. The UE did not provide a response to the plain text message, which could imply that it did not accept or process the unencrypted message. According to the 3GPP standards, after the successful completion of 5G-AKA, NAS messages should be encrypted to protect the integrity and confidentiality of the communication. The fact that the UE did not respond to the unencrypted message could be interpreted as a security measure, adhering to the standard by not engaging with potentially insecure communication. Therefore, based on the UE's lack of response to the plain text message, it appears that the UE acted in a secure manner by not accepting unencrypted communication after the 5G-AKA was completed. Secure</p>
255	255	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 an unencrypted identity request aligns with security best practices, as responding to such a request could expose sensitive information. By not responding, the UE avoids potential security risks associated with transmitting its IMEI in plain text. Therefore, the UE's action of not responding to the unencrypted identity request is consistent with maintaining security as per the 5G standards. Secure</p>

256	256	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 manipulation. 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 invalid or malicious. This behavior aligns with the 3GPP standards, which emphasize the importance of secure communication. Therefore, the UE's action of not responding to the plain text message can be considered secure, as it avoided potential security risks associated with processing unencrypted messages. Secure</p>
257	257	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. The AMF requested the Subscription Concealed Identifier (SUCI) from the UE, but the UE did not respond. According to the 3GPP standards, after the 5G Authentication and Key Agreement (5G-AKA) procedure is completed, all 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 SUCI should not be transmitted without encryption. 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 the risk of 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 refrains from engaging in potentially insecure communication. Secure</p>

258	258	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. According to the 3GPP standards, messages should be encrypted after the 5G-AKA process to maintain confidentiality and integrity. Given that the deregistration request from the AMF was not encrypted, this could be considered a deviation from the expected security practices. Therefore, while the UE's actions in responding to the deregistration request were consistent with the protocol, the lack of encryption in the AMF's message suggests a potential security vulnerability. In conclusion, based on the 3GPP standards, the communication can be considered "Insecure."</p>
259	259	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 GMM status message indicating a 5GMM Cause of 99, which signifies "Information element non-existent or not implemented." Notably, this downlink message from the AMF 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 procedure is completed, NAS messages should be encrypted to maintain confidentiality and integrity. The fact that the AMF sent a plain text message after the 5G-AKA was completed suggests a potential security vulnerability, as the UE should ideally expect encrypted messages to maintain secure communication. The UE's lack of response to the plain text message could be interpreted as a failure to recognize or handle the security anomaly appropriately. Therefore, based on the 3GPP standards, the UE's action in this scenario can be considered insecure, as it did not ensure the expected level of security in its communication with the AMF. Insecure</p>



260	260	<p>This is 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:</p> <p>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)</p> <p>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 requested state) 0.7153670787811279 UE to AMF UplinkNASTransport, Deregistration request (UE originating)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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, indicating that the message was not compatible with the requested state. In response to this, the UE sent a "Deregistration request (UE originating)" message, which suggests that the UE recognized an issue with the received message and took action to deregister from the network. This behavior indicates that the UE was able to detect an anomaly in the communication, likely due to the unencrypted status message, and chose to terminate its 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 communication practices, as it prevents further exposure to potentially insecure interactions. Therefore, the UE's actions can be considered secure. Secure</p>
261	261	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 using the specified cipher and integrity algorithms (128-5G-EA1 and 128-5G-IA2, respectively). 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 the 5G-AKA process, the UE should respond to the security mode command to establish a secure NAS signaling connection. The lack of response from the UE suggests a failure to complete the security procedure, which is critical for ensuring the confidentiality and integrity of the communication. This lack of response could indicate a potential vulnerability or misconfiguration in the UE's handling of security procedures. Therefore, based on the 3GPP standards, the UE's action in this scenario is considered insecure, as it did not adhere to the expected security protocol by failing to respond to the security mode command. Insecure</p>

262	262	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 ciphering algorithm and the lack of encryption in the security mode command indicate a potential vulnerability, as the communication was not protected against eavesdropping. The absence of a response from the UE could suggest a failure to establish a secure connection or a non-compliance with the expected security procedures. Based on these observations, the action taken by the UE was insecure according to the 5G standard outlined by 3GPP. Insecure</p>
263	263	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 unencrypted, which could potentially expose sensitive information to eavesdroppers. The UE's lack of response to the plain-text message suggests that it did not engage in further communication, which could be interpreted as a cautious approach to avoid potential security risks. However, the fact that the UE received and processed an unencrypted message without any apparent error or rejection indicates a potential vulnerability in handling unencrypted communications post-authentication. Therefore, based on the 3GPP standards, the UE's action in accepting a plain-text message after the completion of 5G-AKA is considered insecure, as it does not align with the expected security measures for encrypted communication. Insecure</p>

264	264	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 indicates that the rejection was due to the UE being considered illegal, possibly because of a security or compliance issue. 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, the AMF's registration reject message was sent in plain text, which is a deviation from the expected secure communication protocol. Since the UE did not respond to the plain text message, it adhered to the security protocols by not engaging further in an insecure communication. Therefore, the UE's action of not responding to the plain text message aligns with the 5G security standards, indicating that the UE maintained a secure posture in this interaction. Secure</p>
-----	-----	---	--

265	265_F	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 UE sent a service request, the AMF responded with an authentication request. Notably, the authentication request was sent in plain text, which is unusual as messages should be encrypted after the completion of the 5G Authentication and Key Agreement (5G-AKA) process. The AMF's message included parameters such as ABBA, RAND, AUTN, and ngKSI values. The UE responded with an authentication failure, citing that the ngKSI was already in use. This response indicates that the UE detected a potential security issue, as the ngKSI (NAS key set identifier) should be unique for each security context. The UE's action to reject the authentication request due to the reuse of an ngKSI suggests that it adhered to the 3GPP standards, which require unique security contexts to prevent replay attacks and ensure secure communication. By identifying and rejecting the reuse of an ngKSI, the UE demonstrated a secure response to a potentially insecure situation orchestrated by the AMF during the test. Therefore, the UE's actions were in line with maintaining the integrity and security of the communication as per the 5G standards. Secure</p>
266	266	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, which was sent in plain text. The 5G Authentication and Key Agreement (5G-AKA) procedure was noted as completed prior to this exchange, which is a prerequisite for ensuring that subsequent NAS messages are encrypted. However, the AMF's response was sent in plain text, which is unusual and potentially problematic, as it suggests that the encryption expected after a successful 5G-AKA was not applied. The UE did not provide any response to the authentication reject message. 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's message was sent in plain text indicates a deviation from this standard, but since the UE did not respond to the plain text message, it suggests that the UE did not engage in potentially insecure communication. Therefore, the UE's lack of response to an unencrypted message aligns with secure behavior as per the 3GPP standards, as it avoided further interaction that could compromise security. Secure</p>

267	267	<p>This is 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:</p> <p>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</p> <p>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 0.5201799869537354 AMF to UE SACK (Ack=6, Arwnd=106496) , DownlinkNASTransport, Authentication reject</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, which was sent in plain text. The UE did not provide any response to this message. According to the 3GPP standards, for NAS messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed successfully. In this scenario, the 5G-AKA was completed, yet the AMF sent an authentication reject message in plain text, which is unusual as it should have been encrypted if the 5G-AKA was indeed completed. 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 potentially be a security threat. Therefore, based on the UE's action of not responding to the plain text message, it adhered to secure communication practices as per the 3GPP standards. Secure</p>
268	268	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 test indicates that the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is a prerequisite for ensuring that subsequent NAS messages are encrypted and protected. The downlink message from the AMF was marked as "Protected," but the security header was labeled as "Unknown," and the UE did not provide a response to the configuration update command. According to the 3GPP standards, once the 5G-AKA is completed, NAS messages should be encrypted and integrity protected to ensure secure communication. The lack of a response from the UE could indicate a failure to process the message, possibly due to an issue with the security header or the message's integrity. The absence of a response from the UE raises concerns about its ability to handle protected messages correctly, which is crucial for maintaining secure communication. Therefore, based on the interaction and the UE's lack of response, the action taken by the UE appears to be insecure according to the 5G standard outlined by 3GPP. Insecure</p>

269	269	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 test indicates that the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is a prerequisite for ensuring that subsequent NAS messages are encrypted. However, the "deregistration accept" message from the AMF was sent in plain text, which suggests that the message was not encrypted. According to the 3GPP standards, once the 5G-AKA is completed, NAS messages should be encrypted to protect the integrity and confidentiality of the communication. The UE did not respond to the plain text message, which could imply that it did not accept the unencrypted message, potentially adhering to security protocols. However, the lack of response could also indicate a failure to handle the situation appropriately. Given that the AMF's message was not encrypted and the UE did not provide a response, it raises concerns about the security of the interaction. The UE's lack of response to an unencrypted message could be seen as a cautious approach, but without further context on whether this behavior is intentional and compliant with security protocols, it is difficult to definitively conclude the security posture. Based on the information provided, the interaction appears to be insecure due to the plain text communication and the lack of a clear, secure response from the UE. Insecure</p>
270	270	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. In this scenario, the 5G-AKA was not completed, meaning that the communication was not encrypted. 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 transmitting sensitive information, such as the IMEISV, over an unencrypted channel, which aligns with the security principles of minimizing exposure of sensitive data. Therefore, the UE's action in this context was secure, as it prevented potential interception of sensitive information in an unprotected communication environment. Secure</p>

271	271	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 UE's International Mobile Equipment Identity (IMEI). 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. In this scenario, the 5G-AKA was not completed, which means that the communication was not encrypted. The UE's lack of response to the plain text identity request from the AMF can be considered a secure action. This is because responding to an unencrypted identity request could expose sensitive information, such as the IMEI, to potential interception. By not responding, the UE avoids the risk of disclosing its identity 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 was secure. Secure</p>
272	272	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. Despite the AMF's service accept message being protected, the lack of completion of the 5G-AKA means that the security context was not fully established. Subsequently, the UE sent a deregistration request, indicating that it was originating the deregistration process. The UE's action to deregister without completing the 5G-AKA suggests a potential security vulnerability, as the communication may not have been fully secure. According to the 3GPP standards, the 5G-AKA should be completed to ensure that all subsequent communications are encrypted and secure. Therefore, the UE's action to proceed with deregistration without a completed 5G-AKA indicates a lapse in security protocol adherence. Insecure.</p>

273	273	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 deregistration request to the UE, which was integrity protected and ciphered, indicating that the message was secured. However, the 5G Authentication and Key Agreement (5G-AKA) procedure was not completed, which is a critical step for establishing a secure communication channel. The 5G-AKA is responsible for mutual authentication between the UE and the network and for deriving the keys used for encryption and integrity protection. Since the 5G-AKA was not completed, the security context necessary for protecting NAS messages was not fully established. Despite the AMF's message being protected, the UE did not respond to the deregistration request, which could be interpreted as a lack of proper handling of the message or an indication of an issue in the security procedure. According to the 3GPP standards, the UE should not engage in secure communication without completing the 5G-AKA process, as this ensures that both parties are authenticated and that the keys used for encryption and integrity protection are valid. Therefore, the UE's action of not responding to the deregistration request, given the incomplete 5G-AKA, aligns with maintaining security standards, as it avoids engaging in potentially insecure communication. However, the lack of response could also indicate a failure to handle the situation correctly. Overall, the UE's action in this scenario is considered "Insecure" due to the incomplete 5G-AKA process and the lack of a proper response to the AMF's message.</p>
274	274	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 it was not encrypted because the 5G-AKA process had not been completed. The UE did not respond to the deregistration request. According to the 3GPP standards, for messages to be encrypted, the 5G-AKA process must be completed to establish security keys. Since the UE did not respond to the deregistration request, it suggests that the UE did not proceed with any action that could compromise its security, given that the message was not encrypted. The lack of response from the UE can be considered a secure action because it avoided processing a potentially insecure message. Therefore, based on the interaction and the 3GPP standards, the UE's action was secure. Secure</p>



275	275	<p>This is 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:</p> <p>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</p> <p>The packet capture during the test using wireshark is:  0.0 UE to AMF InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling]  0.0007669925689697266 AMF to UE SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated by the AMF)</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 deregistered due to an "Illegal ME" (Mobile Equipment). Notably, the deregistration request from the AMF was sent as a protected message, with the security header indicating that it was both integrity protected and ciphered. However, the 5G Authentication and Key Agreement (5G-AKA) process, which is crucial for establishing a secure communication channel, had not been completed at this point. This suggests that the security context necessary for encrypting and protecting messages was not fully established. The UE did not respond to the deregistration request, which could be interpreted as a lack of action or an inability to process the message due to the incomplete security setup. According to the 3GPP standards, the UE should not process messages that are not properly secured, especially if the 5G-AKA has not been completed. Therefore, the UE's lack of response can be seen as adhering to security protocols by not engaging with potentially insecure communication. Based on this analysis, the UE's action was secure as it did not proceed with an unverified and potentially insecure message. Secure</p>
276	276	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. The UE did not respond to this command. According to the 3GPP standards, the 5G-AKA procedure must be completed before any NAS messages can be securely encrypted and integrity protected. The absence of a response from the UE to the plain security mode command suggests that the UE did not proceed with an insecure communication, which aligns with the security protocols that require encryption and integrity protection. Therefore, the UE's lack of response to an unprotected message is consistent with maintaining security standards, as it avoids engaging in potentially insecure communication. Secure</p>

277	277	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 to the AMF, which subsequently sent 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 as a protected message with integrity protection, but without encryption, as encryption requires the completion of the 5G-AKA process. The UE did not respond 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, as this could expose the UE to potential security risks. Since the 5G-AKA was not completed, the UE's lack of response to the unencrypted configuration update command aligns with secure behavior as per the 3GPP standards, which prioritize the protection of sensitive information. Therefore, the UE's action in this scenario can be considered secure, as it avoided processing a potentially insecure message. Secure</p>
278	278	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 identity response to the AMF, which then replied with a configuration update command. Notably, this downlink message from the AMF was sent as a plain NAS message, indicating that the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed, as encryption of NAS messages requires the establishment of security keys through 5G-AKA. Following the receipt of the plain configuration update command, the UE responded with a deregistration request, indicating that it chose to disconnect from the network. This action suggests that the UE recognized the security risk of processing a plain NAS message without the protection of encryption and integrity checks, which are essential for secure communication as per the 3GPP standards. By opting to deregister, the UE avoided potential security vulnerabilities that could arise from processing unprotected messages. Therefore, the UE's decision to deregister in response to receiving a plain configuration update command aligns with secure behavior as outlined by the 3GPP standards, which emphasize the importance of completing the 5G-AKA procedure before engaging in secure communication. Secure</p>

279	279	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 accept message. Notably, this downlink message was sent as protected, even though the 5G Authentication and Key Agreement (5G-AKA) procedure had not been completed. The UE did not provide any response to the deregistration accept message. According to the 3GPP standards, for messages to be encrypted and protected, the 5G-AKA procedure must be completed to establish a secure context. Since the 5G-AKA was not completed, the UE's communication was not secure, as it did not ensure that the messages were encrypted and protected as per the standard requirements. The lack of response from the UE to the deregistration accept message further indicates a potential security vulnerability, as the UE should ideally not accept or process protected messages without a secure context being established. Therefore, based on the 3GPP standards, the action taken by the UE was insecure. Insecure</p>
280	280	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 accept message. Notably, this downlink message was sent as protected, even though 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 integrity-protected. Since the 5G-AKA was not completed, the UE should not have been able to process or trust the protected deregistration accept message from the AMF. The UE's lack of response to the deregistration accept message suggests that it did not process the message, which aligns with the expected behavior when the 5G-AKA is incomplete. This indicates that the UE adhered to the security protocols by not engaging in further communication without a secure channel being established. Therefore, based on the 3GPP standards, the UE's action in this scenario was secure. Secure</p>

281	281	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>In the test scenario, the User Equipment (UE) initiated communication with the Access and Mobility Management Function (AMF) by sending an initial registration request. Following this, the AMF responded with a configuration update command, which was sent as a protected message, indicating that it was integrity protected and ciphered with a new security context. However, 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 mutual authentication between the UE and the network and sets up the necessary security keys for encryption and integrity protection. Since the 5G-AKA was not completed, the security context used for protecting the configuration update command was not properly established, which means the UE should not have accepted or processed the message without a valid security context. The UE's lack of response to the configuration update command suggests that it did not process the message, which aligns with the expected behavior according to the 3GPP standards, as processing a message without a completed 5G-AKA would be insecure. Therefore, the UE's action of not responding to the configuration update command without a completed 5G-AKA indicates that it adhered to the security protocols outlined by the 3GPP standards. Secure</p>
282	282	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 integrity protected and ciphered, indicating that the message was sent in a secure manner. However, the 5G Authentication and Key Agreement (5G-AKA) procedure, which is crucial for establishing a secure communication channel, had not been completed at the time of this interaction. The UE did not provide any response to the configuration update command from the AMF. According to the 3GPP standards, for messages to be securely encrypted and integrity protected, the 5G-AKA procedure must be completed first. Since the 5G-AKA was not completed, the UE's lack of response to the AMF's protected message suggests that it did not proceed with processing the message, which aligns with the expected behavior to ensure security. Therefore, the UE's action of not responding to the configuration update command without a completed 5G-AKA can be considered secure, as it prevents potential vulnerabilities from unprotected communication. Secure</p>

283	283	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 uplink message was part of the Non-Access Stratum (NAS) communication, which is crucial for establishing a connection in a 5G standalone 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 essential for establishing a secure communication channel, had not been completed at this point. According to the 3GPP standards, the 5G-AKA process must be completed to ensure that subsequent messages are encrypted and secure. Since the UE did not respond to the service accept message, it indicates that the UE did not proceed with any further actions that could compromise security. However, the fact that the UE sent an initial registration request before the completion of the 5G-AKA process suggests a potential vulnerability, as the communication was not yet secured. Therefore, based on the 3GPP standards, the action taken by the UE in this scenario can be considered insecure, as it engaged in communication without ensuring that the necessary security procedures were in place. Insecure</p>
284	284	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 had not been completed at this point. The UE then sent a deregistration request, originating from the UE itself. According to the 3GPP standards, for messages to be encrypted and secure, the 5G-AKA procedure must be completed to establish a secure context. Since the 5G-AKA was not completed, the communication between the UE and the AMF was not fully secure, as the necessary encryption and integrity protection mechanisms were not in place. The UE's action of sending a deregistration request without a completed 5G-AKA indicates a potential vulnerability, as the communication could be susceptible to interception or tampering. Therefore, based on the 3GPP standards, the action taken by the UE was insecure. Insecure</p>

285	285	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 encrypted, the 5G-AKA must be completed to establish the necessary security context. Since the 5G-AKA was not completed, the <del>(Plaintext)</del> 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 adhered to the security protocols by not engaging in further communication without a completed 5G-AKA, which is a secure behavior according to the 3GPP standards. Therefore, the UE's action in this scenario can be considered "Secure."</p>
286	286	<p>This is 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:</p> <p>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</p> <p>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 TMSI or 5G-TMSI)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 5G Authentication and Key Agreement (5G-AKA) process, which is essential for securing the communication, had not been completed at this point. Subsequently, the AMF sent a downlink message, a GMM status message, which was protected but indicated a 5GMM Cause of 98, meaning "Message type not compatible with the TMSI or 5G-TMSI". The UE did not respond to this message. According to the 3GPP standards, for messages to be encrypted and secure, the 5G-AKA process must be completed first. Since the 5G-AKA was not completed, the communication was not fully secure. The UE's lack of response to the GMM status message could be seen as a failure to handle an unexpected or incompatible message type, which might indicate a security vulnerability. Therefore, based on the 3GPP standards and the incomplete 5G-AKA process, the action taken by the UE was insecure. Insecure</p>

287	287	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, even though 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 respond to the GMM status message. According to the 3GPP standards, the UE should not process or respond to protected messages if the security context has not been established, as this could lead to potential security vulnerabilities. The lack of response from the UE suggests that it correctly identified the absence of a secure context and refrained from processing the message, adhering to the security protocols outlined by 3GPP. Therefore, the UE's action in this scenario can be considered secure, as it did not engage with potentially insecure communication. Secure</p>
288	288	<p>This is 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:</p> <p>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)</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 use of the 5G-EA0 (null) ciphering algorithm, which does not provide encryption. According to the 3GPP 5G standards, for messages to be encrypted, the 5G Authentication and Key Agreement (5G-AKA) procedure must be completed, which was not the case here. The use of a null ciphering algorithm and the failure to complete the 5G-AKA procedure before proceeding with secure communication indicates a lack of adherence to the security protocols outlined by 3GPP. Therefore, the action taken by the UE in this scenario was insecure, as it did not ensure the confidentiality and integrity of the communication as per the 5G standards. Insecure</p>

289	289	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 the requested identity from the UE was the Globally Unique Temporary Identifier (GUTI). 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, which is a potential security risk. The UE's lack of response to the plain text identity request could be interpreted as a security measure to avoid 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 of not responding to the plain text identity request can be considered secure, as it prevents the potential exposure of sensitive information in an unprotected manner. Secure</p>
290	290	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE.  Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes.  For messages to and from the UE to be encrypted, the 5G-AKA must first be completed.  Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP?  Please walk through your thought process before answering.  Please ensure that your response is in a paragraph format.  At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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-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, and the UE's lack of response to the plain text identity request can be seen as a cautious action to avoid exposing sensitive information in an unsecured manner. This behavior aligns with security best practices, as it prevents the potential exposure of the IMEISV in an unprotected communication channel. Therefore, the UE's action of not responding to the identity request in plain text, without the completion of 5G-AKA, can be considered secure. Secure</p>



291	291	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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. 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</p>
292	292	<p>This is 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:</p> <p>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</p> <p>The packet capture during the test using wireshark is: 0.11100292205810547 UE to AMF SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response 0.1112029524597168 AMF to UE SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Deregistration request (UE terminated) (PEI not accepted)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 unauthorized requests, especially when the authentication process is incomplete. However, the fact that the UE did not respond at all could also indicate a potential vulnerability if it was unable to handle such scenarios appropriately. Given that the 5G-AKA was not completed, and the UE did not respond to the deregistration request, the security of the UE's actions is questionable. The UE's lack of response could be interpreted as a cautious approach, but without further context on its intended behavior, it is difficult to definitively conclude its security posture. Therefore, based on the information provided and the 3GPP standards, the UE's actions appear to be insecure due to the incomplete authentication process and lack of response to the deregistration request. Insecure</p>

293	293	<p>This is 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:</p> <p>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</p> <p>The packet capture during the test using wireshark is: 2.651521921157837 UE to AMF UplinkNASTransport, Registration complete, UplinkNASTransport, Deregistration request (UE originated) 2.65175199508667 AMF to UE SACK (Ack=13, Arwnd=106429) , DownlinkNASTransport, Configuration update command</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 "registration complete" message to the AMF, indicating that the initial registration process was successfully concluded. 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, with a security header indicating it was not encrypted (Plain NAS message (0)). 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 ensure confidentiality and integrity. The fact that the AMF sent a plain message and the UE did not respond suggests a potential security vulnerability. The UE's lack of response could indicate that it recognized the message as insecure and chose not to process it, 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. Therefore, the UE's action can be considered "Secure."</p>
294	294	<p>This is 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:</p> <p>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: 303030303030000ee555fb686550000 ngKSI_TSC: Mapped security context ngKSI_KSI: 2 UE provided: No response</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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) process, the UE sent a "security mode complete" message, 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 completion. 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 actions were secure. Secure</p>

295	295	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 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 established. Insecure</p>
296	296	<p>This is 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:</p> <p>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: 313131313131313100133402560000 ngKSI_TSC: Native security context ngKSI_KSI: 2 UE provided: No response</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, 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, once the security context is established, all subsequent NAS messages should be encrypted. The UE's lack of response to the plain-text message aligns with the security protocols, as it avoided engaging in potentially insecure communication. Therefore, the UE's action of not responding to the plain-text message was in accordance with the 5G security standards, demonstrating a secure behavior in this context. Secure</p>

297	297	<p>This is 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:</p> <p>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</p> <p>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)</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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, followed by the AMF sending a "deregistration accept" message. The test indicates that the 5G Authentication and Key Agreement (5G-AKA) process was completed, which is a prerequisite for secure communication. However, the subsequent downlink message from the AMF, "deregistration accept," 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 is completed, all NAS messages should be encrypted to ensure confidentiality and integrity. The fact that the AMF sent a plain text message and the UE did not respond suggests a potential security vulnerability. The UE's lack of response could indicate that it did not recognize or process the plain text message as valid, which might be a security measure to avoid processing unencrypted messages. However, the absence of a response also leaves room for ambiguity regarding the UE's handling of such messages. Given the requirement for encryption post-5G-AKA, the UE's interaction in this scenario appears insecure, as it did not ensure the confidentiality of the communication. Therefore, based on the 3GPP standards, the action taken by the UE was "Insecure."</p>
298	298	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 communications. 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, adhering to the principle of not accepting unencrypted messages after security mode establishment. Therefore, based on the UE's actions, it maintained security by not responding to an unencrypted message after the security mode was supposedly established. Secure</p>

299	299	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 accepted the security parameters and was ready to proceed with 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 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. The UE's lack of response to the plain text "authentication reject" message could be interpreted as a failure to recognize or handle the security anomaly, which might indicate a vulnerability. Based on the 3GPP standards, the UE should have mechanisms to detect and respond to such security breaches. Therefore, the UE's action, or lack thereof, in this scenario appears to be insecure as it did not adequately address the security lapse. Insecure</p>
300	300	<p>This is 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:</p> <p>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</p> <p>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</p> <p>This is a test simulation conducted to explore the security of the tested UE. Focus only on the actions taken by the UE, as we were in control of the AMF for testing purposes. For messages to and from the UE to be encrypted, the 5G-AKA must first be completed. Please summarize the interaction between the UE and the AMF in a short paragraph. Based on your summary of the interaction, Do you think the action taken by the UE was secure or insecure based on the 5G standard outlined by 3GPP? Please walk through your thought process before answering. Please ensure that your response is in a paragraph format. At the end of your response on the following line, state "Secure" or "Insecure" to indicate if the UE was secure or insecure in it's communication.</p>	<p>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 was ready to proceed with secure communication. However, the subsequent message from the AMF was an "identity request" sent in plain text, requesting the Temporary Mobile Subscriber Identity (TMSI) 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 the confidentiality and integrity 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-conscious action, as responding to an unencrypted request could expose sensitive information. Therefore, the UE's decision not to respond to the plain text identity request aligns with maintaining security standards by not engaging in potentially insecure communication. Secure</p>