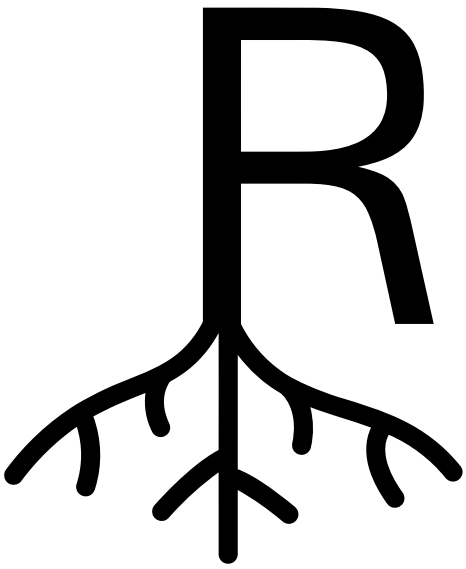
5G SCAS Evaluation
Access and Mobility management Function AMF
3GPP TS 33.512 version 16.3.0 Release 16

Radix Security

05.07.2022



Example Test Report
Sample Core Network Implementation

Contents

1 Test Description

The subset of AMF test cases applied for this evaluation is realistic, and the test results represent actual failure and success evaluations. Due to the use of standard interfaces, the test setup can be transferred to arbitrary core network implementations that expose an IP interface.

1.1 Reference Files

The following files specify the test cases and provide a reference documentation.

- 5G Security Assurance Specification (SCAS): 3GPP TS 33.512 version 16.3.0 Release 16
- 5G Security architecture and procedures for 5G System: 3GPP TS 33.501 version 16.3.0 Release 16
- UMTS/LTE Catalogue of general security assurance requirements: 3GPP TS 33.117 version 16.6.0 Release 16
- 5G threats and critical assets in 3GPP network product classes: 3GPP TR 33.926 version 16.3.0 Release 16
- 5G Non-Access-Stratum (NAS) protocol for 5G System (5GS): 3GPP TS 24.501 version 15.5.0 Release 15
- UMTS/LTE Vocabulary for 3GPP Specifications: 3GPP TR 21.905 version 14.1.1 Release 14

1.2 Setup

The testing setup consists of a core network probe that implements the test cases and provides functions for the standard interfaces, and the AMF as the system under test. The AMF is part of the core network, which is represented by a sample system for the generation of this example test report.

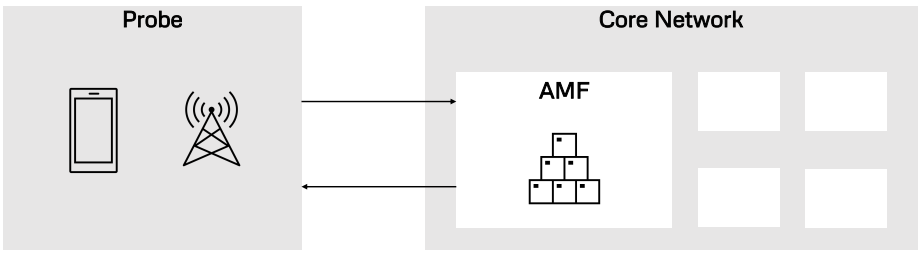
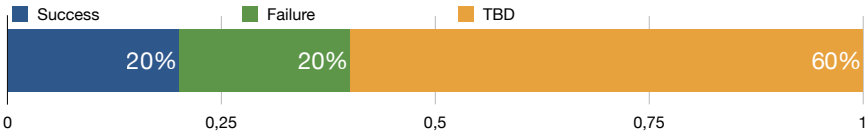


Figure 1: Testing Setup for AMF SCAS

The probe connects to the external IP interface of the core network and directly interacts with the AMF. It involves a UE and gNodeB component without depending on a physical radio connection, which minimizes the impact of noise due to transmission errors.

1.3 Test Statistics

The AMF SCAS tests include a total of 9 tests. The automatic implementation of this exemplary test suite represents 3 out of these 9 test cases, of which 1 is an extended version of a basic test. This results in a total of 10 test cases represented in the implementation. The following summarizes the overall test statistics in which we count the total of 10 cases and compute relative results based on this. Overall, 20 % of test cases succeeded, and 20 % of cases failed. The remaining 60 % of cases are not implemented at the moment and excluded from the statistics. The detailed table documents the amount of succeeded and failed sub-tests within each test case. We document the statistics of the implemented test cases as follows.



Section	Test Case	Passed Combinations	Result
4.2.2.1.2	TC-RES*-VERIFICATION-FAILURE	100% 2/2	Passed
4.2.2.6.1	TC-UE-SEC-CAP-HANDLING-AMF	27% 73% 68/256	Failed
4.2.2.3.3	TC-NAS-INT-SELECTION-USE-AMF	100% 4/4	Passed
4.2.2.3.3+	TC-NAS-INT-SELECTION-USE-AMF+	42% 58% 80/192	Failed

Figure 2: Analysis Statistics

- **4.2.2.1.2** includes 2 different combinations of sub-tests of which all succeeded, leading to a success rate of 100 %.
- **4.2.2.6.1** includes 256 different combinations of algorithms of which 68 sub-tests succeeded. This leads to a success rate of 27 % and an overall failed test.
- **4.2.2.3.3** includes 4 different combinations of which all 4 succeeded leading to a success rate of 100 %.
- **4.2.2.3.3+** is an extended test case that includes all possible combinations of algorithms (instead of the basic sets covered in 4.2.2.3.3). Out of the 192 combinations, 80 sub-tests succeeded leading to a success rate of 80 %.

2 SCAS Results

Section	Test Case	Result
4.2.2.1.2	TC-RES*-VERIFICATION-FAILURE	Passed
4.2.2.6.1	TC-UE-SEC-CAP-HANDLING-AMF	Failed
4.2.2.3.3	TC-NAS-INT-SELECTION-USE-AMF	Passed
4.2.2.3.3+	TC-NAS-INT-SELECTION-USE-AMF+	Failed
4.2.2.1.1	TC-SYNC-FAIL-SEAF-AMF	TBD
4.2.2.3.1	TC-NAS-REPLAY-AMF	TBD
4.2.2.3.2	TC-NAS-NULL-INT-AMF	TBD
4.2.2.4.1	TC-BIDDING-DOWN-XN-AMF	TBD
4.2.2.4.2	TC-NAS-ALG-AMF-CHANGE	TBD
4.2.2.5.1	TC-5G-GUTI-ALLOCATION	TBD

2.1 4.2.2.1.2 TC-RES*-VERIFICATION-FAILURE

2.1.1 SCAS Information

Details: The SEAF shall proceed with step 10 in Figure 6.1.3.2-1 and after receiving the Nausf-UEAuthentication-Authenticate Request message from the AUSF in step 12 in Figure 6.1.3.2-1, proceed as described below: - if the AUSF has indicated in the Nausf-UEAuthentication-Authenticate Response message to the SEAF that the verification of the RES* was not successful in the AUSF, or - if the verification of the RES* was not successful in the SEAF, then the SEAF shall either reject the authentication by sending an Authentication Reject to the UE if the SUCI was used by the UE in the initial NAS message or the SEAF/AMF shall initiate an Identification procedure with the UE if the 5GGUTI was used by the UE in the initial NAS message to retrieve the SUCI and an additional authentication attempt may be initiated. Also, if the SEAF does not receive any Nausf-UEAuthentication-Authenticate Request message from the AUSF as expected, then the SEAF shall either reject the authentication to the UE or initiate an Identification procedure with the UE."

Purpose: 1. Verify that the SEAF/AMF correctly handles RES* verification failure detected in the SEAF/AMF or/and in the AUSF, when the SUCI is included in the initial NAS message. 2. Verify that the SEAF/AMF correctly handles RES* verification failure detected in the SEAF/AMF or/and in the AUSF, when the 5G-GUTI is included in the initial NAS message.

Expected: For test case 1 and 2, the value for RES* in the Nausf-UEAuthentication-Authenticate Request message from the AMF to the AUSF is NULL. For test case 1 and 3, the SEAF/AMF rejects the authentication by sending an Authentication Reject to the UE. For test case 2 and 4, the SEAF/AMF initiates an Identification procedure with the UE to retrieve the SUCI.

2.1.2 Analysis Details

To analyze the RES* Verification Failure, we directly interfere with the MAC of messages sent from the UE to the network. To this end, we test permutations in which the MAC was invalidated on purpose (set to 0), and cases in which the original and correct MAC remained in place. To succeed in the test, the network must reject all messages with an invalid MAC and only accept those that lead to a successful RES* verification.

RES* invalidated	Rejected	Success
True	True	1
False	False	1

Test Result: Passed

2.2 4.2.2.6.1 TC-UE-SEC-CAP-HANDLING-AMF

2.2.1 SCAS Information

Details: If the REGISTRATION REQUEST message is received with invalid or unacceptable UE security capabilities (e.g. no 5GS encryption algorithms (all bits zero), no 5GS integrity algorithms (all bits zero), mandatory 5GS encryption algorithms not supported or mandatory 5GS integrity algorithms not supported, etc.), the AMF shall return a REGISTRATION REJECT message

Purpose: Verify that UE security capabilities invalid or unacceptable are not accepted by the AMF under test in registration procedure.

Expected: The tester captures the Registration reject message sent by AMF under test to the UE.

2.2.2 Analysis Details

We tested 256 individual combinations of UE Security Capabilities. Out of these permutations, 68 combinations succeeded and 188 failed. The different combinations represent all possible permutations of algorithms in the UE Security Capabilities. The table shows a subset of tests including the Algorithms, the accept decision of the AMF (Accepted) and the Expected result. In case of a discrepancy, the sub-test fails (0). If the expected and actual decision match, the sub-test succeeds (1). In total, the test can only succeed if all permutations lead to a matching accept decision.

Algorithms	**Accepted**	**Expected**	**Result**
None	False	False	1
NIA3	False	False	1
NIA2	True	False	0
NIA2, NIA3	True	False	0
NIA1	True	False	0
NIA1, NIA3	True	False	0
NIA1, NIA2	True	False	0
NIA1, NIA2, NIA3	True	False	0
NIA0	False	False	1
NIA0, NIA3	False	False	1

Test Result: Failed

2.3 4.2.2.3.3 TC-NAS-INT-SELECTION-USE-AMF

2.3.1 SCAS Information

Details: The AMF shall then initiate a NAS security mode command procedure, and include the chosen algorithm and UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE (see sub-clause 6.7.2 of the present document). The AMF shall select the NAS algorithm which have the highest priority according to the ordered lists." as specified in TS 33.501 [2], clause 5.5.2.

Purpose: Verify that the AMF selects the NAS integrity algorithm which has the highest priority according to the ordered list of supported integrity algorithms and is contained in the 5G security capabilities supported by the UE. Verify that the selected NAS security algorithm is being used.

Expected: The selected integrity algorithm has the highest priority according to the list of ordered NAS integrity algorithm and is contained in the UE 5G security capabilities. The MAC verification of the Security Mode Complete message is successful.

2.3.2 Analysis Details

We tested 4 individual combinations of UE Security Capabilities. Out of these permutations, 4 combinations succeeded and 0 failed. The results table provides a subset of test results for successful and failed combinations. It documents the UE Security Capabilities (Capabilities) and the algorithms selected and sent in the Security Mode Command (Selected). Furthermore, it shows the configured priority list of integrity algorithsm (Int.) and encryption algorithms (Enc.) from highest to lowest priority. Please note that we use a setup with null encryption NEA0. The priority list is part of the individual configuration of the network and the test fully focuses on the corect selection rather than the security of the configured priority list. Finally, the Failure column documents the reason for the failing test case.

Capabilities	Selected	Int.	Enc.	Failure
All	NEA0, NIA2	2,1,0	0,1,2	None
All	NEA0, NIA2	2,1,0	0,1,2	None
All	NEA0, NIA2	2,1,0	0,1,2	None
All	NEA0, NIA2	2,1,0	0,1,2	None

Test Result: Passed

2.4 4.2.2.3.3+ TC-NAS-INT-SELECTION-USE-AMF+

2.4.1 SCAS Information

Details: The AMF shall then initiate a NAS security mode command procedure, and include the chosen algorithm and UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE (see sub-clause 6.7.2 of the present document). The AMF shall select the NAS algorithm which have the highest priority according to the ordered lists." as specified in TS 33.501 [2], clause 5.5.2.

Purpose: Verify that the AMF selects the NAS integrity algorithm which has the highest priority according to the ordered list of supported integrity algorithms and is contained in the 5G security capabilities supported by the UE. Verify that the selected NAS security algorithm is being used.

Expected: The selected integrity algorithm has the highest priority according to the list of ordered NAS integrity algorithm and is contained in the UE 5G security capabilities. The MAC verification of the Security Mode Complete message is successful.

2.4.2 Analysis Details

We tested 192 individual combinations of UE Security Capabilities. Out of these permutations, 80 combinations succeeded and 112 failed. The results table provides a subset of test results for successful and failed combinations. It documents the UE Security Capabilities (Capabilities) and the algorithms selected and sent in the Security Mode Command (Selected). Furthermore, it shows the configured priority list of integrity algorithsm (Int.) and encryption algorithms (Enc.) from highest to lowest priority. Please note that we use a setup with null encryption NEA0. The priority list is part of the individual configuration of the network and the test fully focuses on the corect selection rather than the security of the configured priority list. Finally, the Failure column documents the reason for the failing test case.

Capabilities	**Selected**	**Int.**	**Enc.**	**Failure**
All	NEA0, NIA2	2,1,0	0,1,2	None
All	NEA0, NIA2	2,1,0	0,1,2	None
NIA1	NEA0, NIA1	2,1,0	0,1,2	Int. Priority
NIA1, NIA3	NEA0, NIA1	2,1,0	0,1,2	Int. Priority
All	NEA0, NIA2	2,1,0	0,1,2	None
All	NEA0, NIA2	2,1,0	0,1,2	None
All	NEA0, NIA2	2,1,0	0,1,2	None
All	NEA0, NIA2	2,1,0	0,1,2	None
NIA0, NIA1	NEA0, NIA1	2,1,0	0,1,2	Int. Priority
NIA0, NIA1, NIA3	NEA0, NIA1	2,1,0	0,1,2	Int. Priority

Test Result: Failed

2.5 4.2.2.1.1 TC-SYNC-FAIL-SEAF-AMF

2.5.1 SCAS Information

Details: Upon receiving an authentication failure message with synchronisation failure (AUTS) from the UE, the SEAF sends an Nausf-UEAuthentication-Authenticate Request message with a "synchronisation failure indication" to the AUSF. An SEAF will not react to unsolicited "synchronisation failure indication" messages from the UE. The SEAF does not send new authentication requests to the UE before having received the response to its Nausf-UEAuthentication-Authenticate Request message with a "synchronisation failure indication" from the AUSF (or before it is timed out)."

Purpose: Verify that synchronization failure is correctly handled by the SEAF or AMF.

Expected: Before receiving Nausf-UEAuthentication-Authenticate Response message from the AUSF and before the timer for receiving Nausf-UEAuthentication-Authenticate Response message runs out. For Test B, the SEAF/AMF does not send any new authentication request to the UE. For Test A, the SEAF/AMF may initiate new authentication towards the UE.

2.5.2 Analysis Details

Test Result: TBD

2.6 4.2.2.3.1 TC-NAS-REPLAY-AMF

2.6.1 SCAS Information

Details: "AMF shall support replay protection of NAS signalling messages between UE and AMF on N1 interface." as specified in TS 33.501 [2], clause 5.5.1.

Purpose: Verify that the NAS signalling messages are replay protected by AMF over N1 interface between UE and AMF.

Expected: The NAS signalling messages sent between UE and AMF over N1 interface are replay protected.

2.6.2 Analysis Details

Test Result: TBD

2.7 4.2.2.3.2 TC-NAS-NULL-INT-AMF

2.7.1 SCAS Information

Details: "NIA0 shall be disabled in AMF in the deployments where support of unauthenticated emergency session is not a regulatory requirement." as specified in TS 33.501 [2], clause 5.5.2

Purpose: Verify that NAS NULL integrity protection algorithm is used correctly.

Expected: The integrity algorithm selected by the AMF in NAS SMC message is different from NIA0. The NAS Security Mode Command message is integrity protected by the AMF.

2.7.2 Analysis Details

Test Result: TBD

2.8 4.2.2.4.1 TC-BIDDING-DOWN-XN-AMF

2.8.1 SCAS Information

Details: In the Path-Switch message, the target gNB shall send the UE's 5G security capabilities received from the source gNB to the AMF. The AMF shall verify that the UE's 5G security capabilities received from the target gNB are the same as the UE's 5G security capabilities that the AMF has locally stored. If there is a mismatch, the AMF shall send its locally stored 5G security capabilities of the UE to the target gNB in the Path-Switch Acknowledge message. The AMF shall support logging capabilities for this event and may take additional measures,such as raising an alarm.

Purpose: Verify that bidding down is prevented by the AMF under test in Xn handovers.

Expected: The tester captures the Path-Switch Acknowledge message sent by AMF under test to the target gNB, which includes the locally stored 5G security capabilities in the AMF under test for that UE. The tester verifies that a log entry showing the capability mismatch is logged.

2.8.2 Analysis Details

Test Result: TBD

2.9 4.2.2.4.2 TC-NAS-ALG-AMF-CHANGE

2.9.1 SCAS Information

Details: If the change of the AMF at N2-Handover or mobility registration update results in the change of algorithm to be used for establishing NAS security, the target AMF shall indicate the selected algorithm to the UE as defined in Clause 6.9.2.3.3 for N2-Handover (i.e., using NAS Container) and Clause 6.9.3 for mobility registration update (i.e., using NAS SMC). The AMF shall select the NAS algorithm which has the highest priority according to the ordered lists (see sub-clause 6.7.1.1 of the present document).

Purpose: Verify that NAS protection algorithms are selected correctly.

Expected: For Test case 1, the tester captures the NASC of the NGAP HANDOVER REQUEST message sent by the AMF under test to the gNB, which includes the chosen algorithm. For Test case 2, the AMF under test initiates a NAS security mode command procedure and includes the chosen algorithms.

2.9.2 Analysis Details

Test Result: TBD

2.10 4.2.2.5.1 TC-5G-GUTI-ALLOCATION

2.10.1 SCAS Information

Details: A new 5G-GUTI shall be sent to a UE only after a successful activation of NAS security. The 5G-GUTI is defined in TS 23.003 [4]. Upon receiving Registration Request message of type "initial registration" or "mobility registration update" from a UE, the AMF shall send a new 5G-GUTI to the UE during the registration procedure. Upon receiving Registration Request message of type "periodic registration update" from a UE, the AMF should send a new 5G-GUTI to the UE during the registration procedure. Upon receiving Service Request message sent by the UE in response to a Paging message, the AMF shall send a new 5G-GUTI to the UE. This new 5G-GUTI shall be sent before the current NAS signalling connection is released.

Purpose: Verify that a new 5G-GUTI is allocated by the AMF under test in these scenarios accordingly.

Expected: For Test case 1, 2, 3, the tester retrieves a new 5G-GUTI by accessing the NAS signalling packets sent by the AMF under test over N1 interface during registration procedure. For Test case 1, 2, 3, the NAS message encapsulating the new 5G-GUTI is confidentiality and integrity protected by the AMF under test using the NAS security context, which is same as the UE's NAS security context. The new 5G-GUTI is different from the old 5G-GUTI.

2.10.2 Analysis Details

Test Result: TBD