Tests definitions

Table of Contents

Test case #13888 ATNA_SA-SN_ITI19_Error_Cases

Test Summary

Keyword : ATNA_SA-SN_ITI19_Error_Cases_CTS
Name : ATNA_SA-SN_ITI19_Error_Cases
Version : 1.1
Author : vhofman
Date of last 2024-01-26 16:13:50.127945 by vhofman

Type : conformity assessment
Peer Type : NO_PEER_TEST
Status : ready
Verified by : Not verified

Short Description : Verify Secure Application or Secure Node acting as Server are able to reject invalid TLS handshakes

Test Description

Special Instructions

This test exercises several error cases. Gazelle Security Suite acts as a simulated client, trying to connect to a Secure Node (SN) or Secure Application (SA) acting as a server.

****If your SN/SA is only a client** (*ie* it only initiates transactions), **then this test case is not applicable for you.**

To perform this test, your digital certificate must be set up on your system.

If your system is using the SNI extension, a tool dedicated to SNI extension testing is used instead of Gazelle Security Suite error test cases.

Please get in touch with a monitor to obtain informations about how to use this tool.

Description

1. Log in to Gazelle Security Suite. Use the same username/password as for Gazelle Test Management
2. Select menu ***TLS/SSL > Testing > Tests cases***
3. Run each of the error test cases listed:
   - IHE_ErrorCase_Corrupted
   - IHE_ErrorCase_Expired
   - IHE_ErrorCase-Self-Signed
   - IHE_ErrorCase_Unknown
   - IHE_ErrorCase_Without_Authentication
   - IHE_ErrorCase_Wrong_Key

   Once you are on the 'Run a test' page, select your application type (HL7v2, WEBSERVICE or SYSLOG), input the host / IP address and port of your system and click on 'Run'. If you implement several of those application type, you should mix message types over those error test cases in order to have all implemented protocol covered by at least one step.

4. After each test case, find your result in the list of Test Executions.
5. Capture the permanent links to your results. Copy/paste the links into the according testing step using the "Add an URL" button.

When you added evidences for all test cases, change the status of the test to "**To be verified**".

Evaluation

Each TLS error case must have the test verdict of '**PASSED**'. *Note that If TLS sub-verdict that are optional get the verdict '**FAILED**', you can consider it as a warning and not an error.*

In each TLS test result :

- the SUT host must be the IP specified in the configuration of the system.
- the SUT port must be the one specified in the configuration of the system for the protocol.

Each application type (WEBSERVICE, SYSLOG, ...) implemented by your system must have been tested at least one time in those error cases.

Special evaluation - Microsoft:

For some security provider, certificate validation is performed after the handshake (eg Microsoft SSL Engine). In this case, Gazelle Security Suite will mark the tests '**FAILED**'. Monitor must **manually** analyze the connection :

- The handshake must be failed OR a '403 forbidden' message must have been received by the simulator if the application layer is an HTTP web-service.
- If the handshake failed, the simulator must have received a close_notify or a fatal alert.
- the SUT host must be the IP specified in the configuration of the system.
- the SUT port must be the one specified in the configuration of the system for the protocol.

Special evaluation - SNI:

If the vendor's system is using the SNI extension for TLS tests, the logs obtained by using the SNI extension library have to be provided by the monitor, as an evidence attached to all steps requiring evidence.

The reason of the alert message of each result below may slightly differ from the one provided. However, the main validation criteria is that the handshake is interrupted by the server and a close_notify or a fatal alert has been received.

All the test cases located in TLS with the SNI tool may fail with the following respective logs :

Unknown certificate :

140416339390912:error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca:../ssl/record/rec_layer_s3.c:1528:SSL alert number 48

Corrupted certificate :

140078889611712:error:1409441B:SSL routines:ssl3_read_bytes:tlsv1 alert decrypt error:../ssl/record/rec_layer_s3.c:1528:SSL alert number 51

Expired certificate :

140246863073728:error:14094415:SSL routines:ssl3_read_bytes:sslv3 alert certificate expired:../ssl/record/rec_layer_s3.c:1528:SSL alert number 45

Self-signed certificate :

140710334378432:error:14094418:SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca:../ssl/record/rec_layer_s3.c:1528:SSL alert number 48

No authentication :

139964106043840:error:14094410:SSL routines:ssl3_read_bytes:sslv3 alert handshake failure:../ssl/record/rec_layer_s3.c:1528:SSL alert number 40

Test Participants

Role in test : GAZELLE_SECURITY_SUITE (Tool)	Option : R	Nb of instances : 1

Test Participants

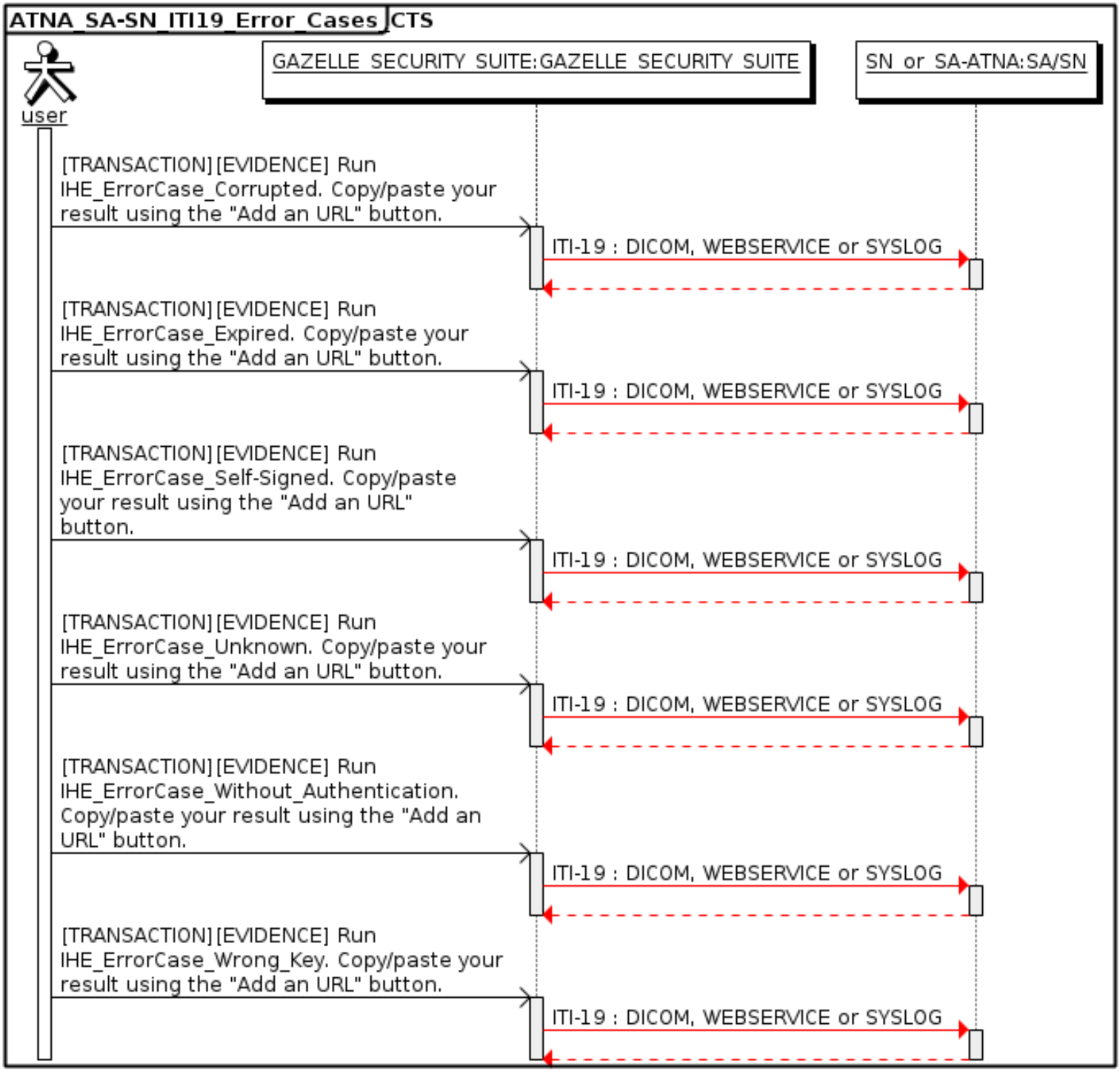
Role in test : SN_or_SA-ATNA (SUT) **Option :** R **Nb of instances :** 1

Actor	Profile	Option
SA	ATNA	NONE
SN	ATNA	NONE

Test Steps

Index	Initiator	Responder	Transaction	Message Type	Secured ?	Option	Description
10	GAZELLE_SECURITY_SUITE	SN_or_SA-ATNA	ITI-19	DICOM, WEBSERVICE or SYSLOG	Yes	Required	
[TRANSACTION][EVIDENCE] Run IHE_ErrorCase_Corrupted. Copy/paste your result using the "Add an URL" button.							
20	GAZELLE_SECURITY_SUITE	SN_or_SA-ATNA	ITI-19	DICOM, WEBSERVICE or SYSLOG	Yes	Required	
[TRANSACTION][EVIDENCE] Run IHE_ErrorCase_Expired. Copy/paste your result using the "Add an URL" button.							
40	GAZELLE_SECURITY_SUITE	SN_or_SA-ATNA	ITI-19	DICOM, WEBSERVICE or SYSLOG	Yes	Required	
[TRANSACTION][EVIDENCE] Run IHE_ErrorCase_Self-Signed. Copy/paste your result using the "Add an URL" button.							
50	GAZELLE_SECURITY_SUITE	SN_or_SA-ATNA	ITI-19	DICOM, WEBSERVICE or SYSLOG	Yes	Required	
[TRANSACTION][EVIDENCE] Run IHE_ErrorCase_Unknown. Copy/paste your result using the "Add an URL" button.							
60	GAZELLE_SECURITY_SUITE	SN_or_SA-ATNA	ITI-19	DICOM, WEBSERVICE or SYSLOG	Yes	Required	
[TRANSACTION][EVIDENCE] Run IHE_ErrorCase_Without_Authentication. Copy/paste your result using the "Add an URL" button.							
70	GAZELLE_SECURITY_SUITE	SN_or_SA-ATNA	ITI-19	DICOM, WEBSERVICE or SYSLOG	Yes	Required	
[TRANSACTION][EVIDENCE] Run IHE_ErrorCase_Wrong_Key. Copy/paste your result using the "Add an URL" button.							

Sequence Diagram



Test case #13889 ATNA_SA-SN_ITI-20

Test Summary

Keyword : ATNA_SA-SN_ITI-20_CTS
Name : ATNA_SA-SN_ITI-20
Version : 1.0
Author : vhofman
Date of last 2024-01-26 16:14:08.408292 by vhofman

Type : conformity assessment
Peer Type : NO_PEER_TEST
Status : ready
Verified by : Not verified

Short Description : Verify a Secure Application or a Secure Node is able to send an Audit Message with the Syslog protocol to the Syslog Collector simulator

Test Description

Special Instructions

This test is run against the Syslog Collector tools, embedded in **Gazelle Security Suite**. UDP and TCP-TLS ports on which the tool is listenning are available to the user on the page **Audit Trail > Syslog Collector**.

Description

This is a test of transaction ITI-20 Record Audit Event.

As a Secure Node or Secure Application, you will generate audit messages in association with various IHE transactions and potential with other system activities (*eg*: system start/stop).

In this test, you must configure your system to send audit messages to the Syslog Collector, acting as an Audit Record Repository. Then trigger any event that initiate an audit message. Your system should finally send the message to the Syslog Collector.

Go to **Gazelle Security Suite**, on page **Audit Trail > Syslog Collector**. Filter the list of received messages by the host or the IP of the sender, and find the message sent according to the timestamps. Click on the magnifying glass to display the message details, then copy its permanent link in the corresponding [EVIDENCE] test step.

After the audit message permanent link is copied , mark the test as to be verified. The monitor will check that everything went right.

Evaluation

The monitor will check that an audit message has been received from the system under test and that the protocol is correctly implemented. This test does **not** verify the validity of the audit-message.

If there is a message, a message content, no errors and RFC5424 parsing is succeed, then the test is successful.

Test Participants

Role in test : GAZELLE_SECURITY_SUITE (Tool) **Option :** R **Nb of instances :** 1

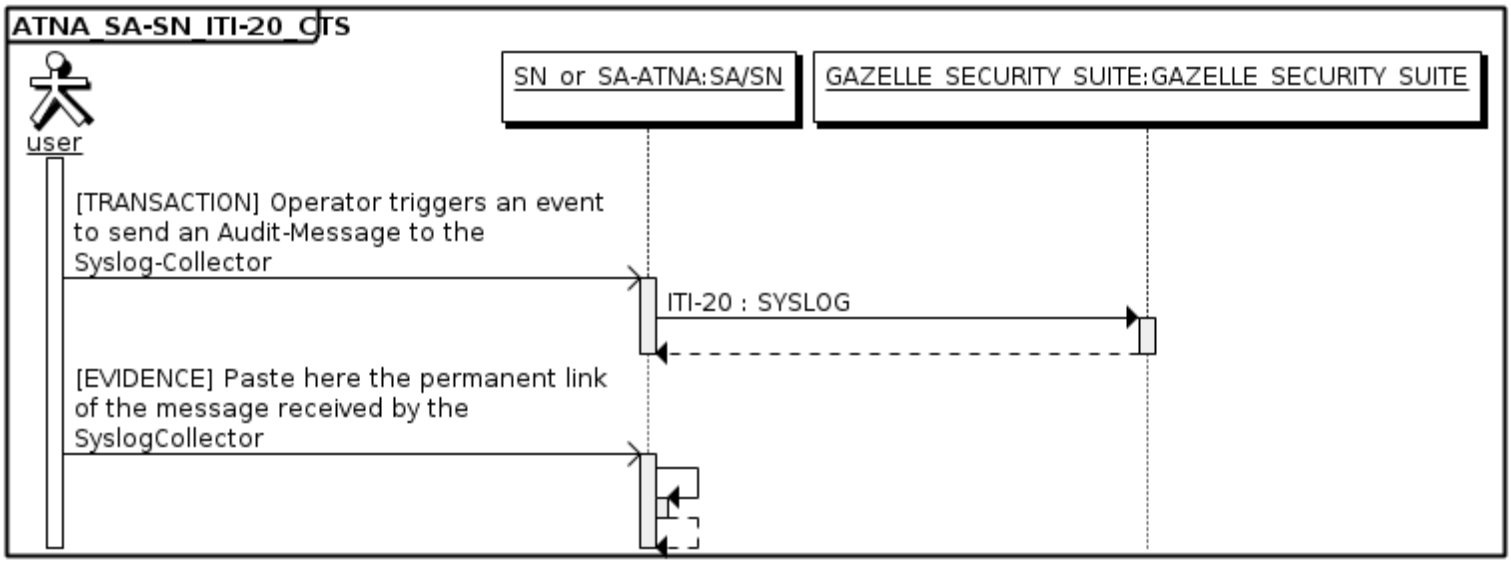
Role in test : SN_or_SA-ATNA (SUT) **Option :** R **Nb of instances :** 1

Actor	Profile	Option
SA	ATNA	NONE
SN	ATNA	NONE

Test Steps

Index	Initiator	Responder	Transaction	Message Type	Secured ?	Option	Description
10	SN_or_SA-ATNA	GAZELLE_SECURITY_SUITE	ITI-20	SYSLOG	No	Required	
[TRANSACTION] Operator triggers an event to send an Audit-Message to the Syslog-Collector							
20	SN_or_SA-ATNA	SN_or_SA-ATNA		None	No	Required	
[EVIDENCE] Paste here the permanent link of the message received by the SyslogCollector							

Sequence Diagram



Test case #13890 ATNA_SA-SN_Questionnaire

Test Summary

Keyword :	ATNA_SA-SN_Questionnaire_CTS	**Type :**	conformity assessment
Name :	ATNA_SA-SN_Questionnaire	**Peer Type :**	NO_PEER_TEST
Version :	1.1	**Status :**	ready
Author :	vhofman	**Verified by :**	**Not verified**
Date of last	2024-01-26 16:14:22.680295 by vhofman		

Short Description : ATNA Secure Application or Secure Node completes the ATNA Questionnaire to provides informatio
on secured elements of the system.

Test Description

Description

This test enables you to describe your system's implementation of the ATNA Secure Application (SA) or Secure Node (SN) actor.

You must complete this test before performing the other ATNA tests. The contents of the questionnaire help us evaluate your system during other tests.

Instructions

1. The ATNA questionnaire resides in Gazelle-Security-Suite.
   - Go to: https://ehealthsuisse.ihe-europe.net/gss and log into the application
   - Select menu *Audit Trail --> ATNA Questionnaire*
2. First, search for any existing questionnaires for your organization. Use the filters at the top of the page to search based on various criteria. If no questionnaire is available for your test system, you need to create a new one.
   - Click on the "New ATNA Questionnaire" button
   - From the dropdown list, select the name of your test system. *Note: If your system doesn't appear, is your test system registered with status of "Completed"?*
   - Save the questionnaire just created and quit it.
3. Complete the questionnaire. Open your Questionnaire with the Editor.
   - In the System details, identify the ATNA actor you support. Choose either "Secure Node (SN)" or "Secure Application (SA)"
   - Complete the "Inbound network communications" tab
   - Complete the "Outbound network communications" tab
   - Complete the "Authentication process for local users" tab
   - Review which Audit messages your system is supporting in "Audit Messages" tab. This tab can completed later on, using other test to trigger every events
   - Complete the "Non network means for accessing PHI" tab - *Only for Secure Nodes (SN)*
   - Complete the "TLS Tests" tab. For instructions on how to run those tests, read the details instructions on the "TLS tests" tab on your questionnaire.(**take notice of the SNI extension part if your system is using it and please get in touch with a monitor to obtain informations about how to use it**)

When all tables are completed (including **ALL** audit-messages are uploaded), set the Questionnaire's status to "Ready for review" in the "Questionnaire details" section. Finally, copy and paste the permanent link to that questionnaire in the dedicated test step.

Evaluation

Certification monitors will review this questionnaire and refer to your answers during other ATNA tests.

Inbound / outbound communication

The monitor will review any comment made on those boundaries:

- Some transaction may be declared "not implemented", then the monitor will verify if such declaration are legitimate (transaction may be required by an implemented profile) and eventually raise a potential warning to the test session manager.
- Transaction declared non secured MUST NOT convey any patient information (PHI).

Local user authentication

Local user authentication process must be described, how many authentication factors are used and which ones.

There is no more evaluation criteria. This is a declarative description.

Audit messages

- Every event triggered by a transaction conveying PHI (and secured) must be supported
- For each supported audit event, an audit-message sample generated by the SUT must have been uploaded
- All uploaded samples must have been validated PASSED

Other means for accessing PHI

Only required for Secure Nodes. The security and privacy strategy must be described for the entire system stack (application to hardware).

- Other PHI possible access
- Means set up for controlling or preventing those access
- Extra audit messages associated to the control of the stack

There is no more evaluation criteria. This is a declarative description.

TLS Tests

- All secured boundaries per type must have been tested against TLS simulators
- The connection must succeed ("blue circle" on page with connection details)
- The cipher suite used must be TLS_RSA_WITH_AES_128_CBC_SHA
- The agreed protocol must be TLSv1.2

The monitor may choose to ask the vendor to re-run a test if the results raise questions about the system's support TLS.

SNI Extension

If the vendor's system is using the SNI extension for TLS tests, the logs obtained by using the SNI extension tool have to be provided by the monitor, as an evidence attached to step 70.

Monitor must make sure that :

- All secured boundaries per type must have been tested against TLS simulators using this tool.
- The connection must succeed.

  Logs must contain on server and client side :

  "Acceptable client certificate CA names
  C = CH, O = IHE, CN = ehealthsuisse.ihe-europe.net CA
  Client Certificate Types: RSA sign, DSA sign, ECDSA sign
  SSL handshake has read 3581 bytes and written 2722 bytes
  Verification: OK".
- The cipher suite used must be TLS_RSA_WITH_AES_128_CBC_SHA (AES128-SHA in OpenSSL).

  Logs must contain on both sides : "CIPHER is AES128-SHA".
- The agreed protocol must be TLSv1.2.

  Logs must contain on client side : "SSL-Session: Protocol : TLSv1".

Test Participants

Role in test : SN_or_SA-ATNA (SUT) **Option :** R **Nb of instances :** 1

Actor	Profile	Option
SA	ATNA	NONE
SN	ATNA	NONE

Test Steps

Index	Initiator	Responder	Transaction	Message Type	Secured ?	Option	Description
10	SN_or_SA-ATNA	SN_or_SA-ATNA		None	No	Required	
[OTHER_ACTION] Set the supported actor in the Questionnaire (SA or SN)							
20	SN_or_SA-ATNA	SN_or_SA-ATNA		None	No	Required	
[OTHER_ACTION] Complete the "Inbound network communications" tab							
30	SN_or_SA-ATNA	SN_or_SA-ATNA		None	No	Required	
[OTHER_ACTION] Complete the "Outbound network communications" tab							
40	SN_or_SA-ATNA	SN_or_SA-ATNA		None	No	Required	
[OTHER_ACTION] Complete the "Authentication process for local users" tab							
50	SN_or_SA-ATNA	SN_or_SA-ATNA		None	No	Required	
[OTHER_ACTION] Complete the "Audit messages" tab							
60	SN_or_SA-ATNA	SN_or_SA-ATNA		None	No	Optional	
[OTHER_ACTION] Complete the "Non network means for accessing PHI" tab (Mandatory for Secure Nodes)							
70	SN_or_SA-ATNA	SN_or_SA-ATNA		None	No	Required	
[OTHER_ACTION] Complete the "TLS Tests" tab							
80	SN_or_SA-ATNA	SN_or_SA-ATNA		None	No	Required	
[EVIDENCE] Paste in this step the permanent link of the ATNA Questionnaire							

Sequence Diagram