KEREVAL
4 rue Hélène Boucher
Z.A Bellevue
35 235 THORIGNE FOUILLARD - FRANCE
Tél. : +33 (0) 223 203 664
RCS : B 442 789 210
APE : 722 C

KEREVAL HEALTHLAB - Project IHE EUROPE

User Guide

GAZELLE SECURITY SUITE – 5.x.x

Version : 2.04

Date: 04/09/2014

Author: Thomas DOLOUE

Function: Quality Assistant

Reference:
KER3-MAN-HEALTHLAB-GSS_USER_GUIDE-2.04

Status: approved

KEREVAL Approval

Name	Function	Date	Visa
Eric POISEAU	Lab Manager	30/03/2015	OK
Anne-Gaëlle BERGE	Quality Manager	05/02/2016	OK

Diffusion

Internal	Recipient	Date	Exemplary
KEREVAL	HealthLab	30/03/2015	Electronic version

External	Recipient	Date	Exemplary
GSS users		30/03/2015	Electronic version

Document history

Version	Date	Author	Modifications
V0.01	02/09/2014	Thomas DOLOUE	Creation
V1.01	04/09/2014	Thomas DOLOUE	For review
V1.02	04/09/2014	Eric POISEAU	Approve
V2.01	30/03/2015	Raphaëlle BATOGE	Enlarge the scope of the documentation to GAZELLE ATNA tool: chapters PKI and ATNA questionnaire are entirely added. TLS chapter is also entirely updated, to map with its new usage. For readability purpose, the changes haven’t been tracked in the content of the document. Document reviewed by Cédric Eoche-Duval and approved by Eric Poiseau
V2.02	04/02/2016	Cédric EOCHE-DUVAL	Update document with new tool name: Gazelle Security Suite. Add paragraph about: double CAS login, ATNA Questionnaire and TM synchronization. Update picture and menu paths.
V2.03	04/02/2016	Cédric EOCHE-DUVAL	For review

V2.04	05/02/2016	Anne-Gaëlle BERGE	Reviewed and approved

Table of content

1 GAZELLE SECURITY SUITE – User guide

The Gazelle Security Suite (GSS) gathers several tools dedicated to the testing of the ATNA profile. It embeds several modes:

- A Public Key Infrastructure to share trusted certificates and associated key pairs for testing purpose.
- A TLS simulator that will simulate clients and servers that can establish secured connection with your system under test (SUT), especially for ATNA profile.
- The ATNA Questionnaire.

This user manual covers each mode.

1.1 Log in

In mostly case, you will have to be logged in to perform actions in GSS. To do so, click on the " Login" button (top right), and input your testing session credentials.

GSS can be linked to several user databases. Whether so, there will be several login buttons. Choose the button with the title that matches the location where you are registered.

2 ATNA questionnaire

2.1 Purpose of the ATNA Questionnaire

The purpose of the ATNA questionnaire is to collect information regarding the implementation of the ATNA requirements in a test system.

Each test system that supports the ATNA Secure Node or Secure Application actor is required to complete an ATNA questionnaire; this is the test named pre-Connectathon test 11106. Your completed questionnaire will help the testing team understand your system's capabilities, and it will direct their evaluation of your system during the test session.

2.2 How to access the ATNA Questionnaire (for connectathon participants)

To find the questionnaire: The ATNA questionnaire resides in GSS, go to `Audit Trail` > `ATNA Questionnaires`.

For instructions on completing the questionnaire, see pre-Connectathon test 11106.

It is important to note that the ATNA Questionnaire build the list of inbound/outbound connections available for your system at its creation and based on your system registration information in Gazelle Test Management. If you modify the AIPOs of your system in TM afterwards, ATNA Questionnaire will no longer be valid. You will have to delete your questionnaire and recreate a new one.

3 PKI : Public Key Infrastructure

Gazelle platform offers its own public key infrastructure: Gazelle PKI. The main use case of this component of GSS is the delivery of signed certificates (and its associated key pair) to all registered participant for a testing session. All theses certificates are issued by a common certification authority (CA), and participant will just have to add this CA to their trust-store. It is the easier way to set up a trusted cluster dedicated to secured connection testing. Out of this cluster, certificates have no value. Also, PKI provide certificates to the TLS simulator that can be used in any other testing purpose. Finally, PKI comes with a certificate validator accessible through the user interface and through a Web Service.

In the case of the European connectathon, generated certificates are signed by the IHE Europe certification authority.

In the case of the Conformity Assessment sessions, generated certificates are signed by a dedicated certification authority (IHE-EUROPE-CATS; conformity-assessment-testing.ihe-europe.net).

3.1 Certificate request

Users can request a certificate for testing :

1. Once logged, go to "PKI" > "Request a certificate"
2. Fill out the form, following fields are required to be provided :
   - Certificate type : basic
   - the country (from the drop-down list)
   - the organization
   - the common name (system keyword is OK)
3. Finally, hit the "request" button.

Then tool administrators are informed and will process it shortly. To retrieve your request and check its status, go to "Certificates" > "List Certificate requests".

If the request is accepted, the certificate will be generated and signed by the certificate authority of the tool. Finally a notification will be sent to your profile in Gazelle Test Management. You will be able to find the certificate in the list of all certificates "PKI" > "List Certificates", or associated with the request in the list of all requests "PKI" > "List certificate requests".

Depending of the configuration of the tool, certificates can also be immediately signed without administration review. Whether it's the case, you will be redirected to the newly created certificate.

Certificates can be downloaded in various format: PEM and DER. The key pair (private and public) of the certificate you have request for is also available in PEM.

Note that you can also generate a keystore in p12 and JKS (java keystore) formats.

3.2 Certificate Validator

Gazelle PKI tool also embeds a certificate validator. You can thus check the conformity of your certificates against several profiles.

1. Go to "PKI" > "Certificate validation".
2. Load the certificate in PEM/CRT format,

3. then select a context and a validator.

Each available validator uses the basic certificate validator first and then validate the certificate against specific rules.

1. Revocation can also be verified.
2. Click on "Validate" to execute the validation.

The result will be displayed on the page. Gazelle Security Suite does not store any validation result.

Certificate validation can also be used from EVSClient (http://gazelle.ihe.net/EVSClient/). Certificate validators are filtered by context and are dispatch over the menu. The advandage of using EVSClient is the generation of a validation report and its permanent storage.

3.3 Request a certificate for Gazelle Single-Sign on service

Gazelle platform has a single-sign on service in order to prevent the user to create a new login in each of the tools offered by the testbed. Read more about this service at : http://gazelle.ihe.net/content/gazelle-single-sign-authentication-users

In each of the tools offered by Gazelle platform, when you use the "CAS login" link, you are asked to provide your CAT credentials. In order to bypass the entering of your credentials, you can, in some Internet browser, import a certificate which will be used to silently authenticate yourself.

To generate this certificate, go to "PKI" > "Install browser certificate for CAS auto-login". Also read http://gazelle.ihe.net/content/cas-autologin

4 SSL / TLS Simulators

The TLS mode gathers two functionalities: the simulators and the connection testing. While simulators can be used to perform exploratory testing, the connection testing provides a more rigorous environment where test cases are defined and expect specifics results.

4.1 Simulators

The simulator is used to effectively test the establishment of a secured connection. It can simulate both side of a connection: client or server. And those simulators are fully tunable by the administrator of the tool. Here is some example of parameters:

- supported protocols
- supported ciphersuites
- Client side authentication required or not.
- Certificate used
- Trusted certificate authorities
- Revocation checking

Once the simulators are set up, they can be used by any logged user for testing. Running a client is equivalent to do a "secured" ping on a target, while server is a listening channel for connection attempts.

The TLS simulator relies on a dedicated instance of the Gazelle Proxy to intercept messages. It offers a shortcut to validate the message content with EVSClient tool.

Each time a connection attempt is done, whatever the client side or server side it is, a secured connection summary is recorded and is added to the connection list. It informs users about the result of the security negotiation (also called handshake). A blue circle indicates the negotiation has succeeded, and a red circle the negotiation has failed. Details on this connection can be displayed for a better understanding.

4.1.1 Using clients simulators

To initiate a secured connection with a SUT that acts as server, simulated clients can be used. Go to "SSL / TLS" > "Simulators" > "Clients". You will see the list of all available clients. Chose one of them and click on "Start a test". On this new page all TLS parameters for this simulator will be sum up. Verify it address your needs. Simulated client are not dependent on the application message, so you can select the desired kind of message to send. Here is the list of supported application protocol:

- DICOM_ECHO
- HL7
- WEBSERVICE
- SYSLOG
- RAW

Finally input the targeted host and port of your SUT and click on "Start client". The connection attempt will be recorded and displayed below the "Start client" button.

Sometimes connections take a bit more time than expected and are not immediately displayed. In this case, try to refresh the page.

4.1.2 Using server simulators

Server simulators are permanently listening. To test your SUT acting as a client, you just have to choose one of the available and running servers in the list "SSL / TLS" > "Simulators" > "Servers", note its IPaddress (or host) and port and send a message to it with your system. Connections will be recorded, go to "Access logs" or in the "View" page to list them.

In fact, server simulators are just channels that forward the message to a real server. If an answer is expected to your message, pay attention to select a server that forwards to a system that can effectively understand the content of your message. It is usually indicated in the keyword of the simulator.

Sometimes connections take a bit more time than expected and are not immediately displayed. In this case, try to refresh the page.

4.2 Secured connection testing

Since EU-CAT 2015, a set of test scenario has been set up to increase the TLS negotiation testing part. There are two goals:

- Make easier the graduation of the Authentication testing for the monitors
- Perform error case scenarios to stress the system under test and get a better trust level.

For now, only the systems acting as responder (servers) can run these scenarios.

4.2.1 Test cases overview

go to "SSL / TLS" > "Testing" > "Test Cases". You will see the list of available test cases. For each test, a short description presents the goal of the scenario. In the detailed view, all the parameters that will be used during the test and its expected result are summarized.

At the bottom of the page, all the test instances are recorded. You can apply filters on the list to help you to find your results. To view the detail of a test run, click on the magnifying glass.

4.2.2 Run a test

To run a test, you must previously add the IHE Europe CA certificate to your trust-store.

Click on the "Run" button of the test of your choice. The TLS negotiation tests are not dependent on the application message, so you can select the desired kind of message to send. Here is the list of supported application protocol:

- DICOM_ECHO
- HL7
- WEBSERVICE
- SYSLOG
- RAW

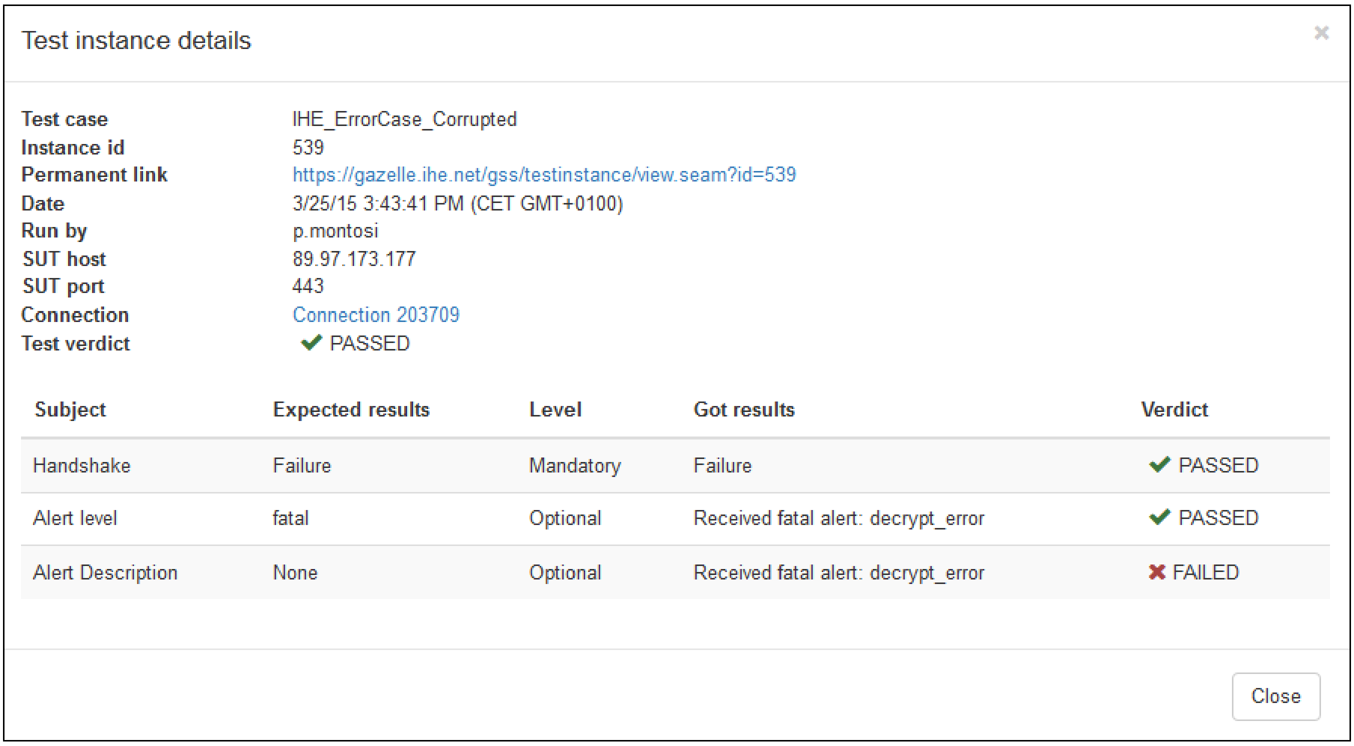
Finally input the targeted host and port of your SUT and click on "Run the test". The test instance will be recorded and displayed below.

Sometimes, the TLS Simulator is not initiated and the test instance is marked "NO RUN". In this case, re-launch the test.

4.2.3 Understand the verdict

The verdict of a test is determined according to 3 sub-verdicts: the handshake verdict, the alert level verdict, and the alert description verdict. Some of these sub-verdicts can be declared as optional while the others are required. To be PASSED, a test must have all its required verdicts to PASSED.

An optional element will not be taken into account to calculate the final test verdict and you can consider this element as a warning. Here is an example, where the alert received was a 'certificate unknown':



Test instance details

Test case	IHE_ErrorCase_Corrupted
Instance id	539
Permanent link	https://gazelle.ihe.net/gss/testinstance/view.seam?id=539
Date	3/25/15 3:43:41 PM (CET GMT+0100)
Run by	p.montosi
SUT host	89.97.173.177
SUT port	443
Connection	Connection 203709
Test verdict	✓ PASSED

Subject	Expected results	Level	Got results	Verdict
Handshake	Failure	Mandatory	Failure	✓ PASSED
Alert level	fatal	Optional	Received fatal alert: decrypt_error	✓ PASSED
Alert Description	None	Optional	Received fatal alert: decrypt_error	✗ FAILED

In error test cases, the Handshake is usually expected to be FAILED. However it is not the only requirement! The simulator expects to receive a fatal/warning alert or a close_notify from the targeted system. If the connection is closed without receiving those alert messages, the Handshake verdict will be failed. *For more information about ending a TLS negotiation and error alerts, see RFC 2246 section 7.2.*

4.3 Tips

4.3.1 TLS renegociation

Mostly with IIS servers (Microsoft HTTP server), some resources may be protected. So other a single TLS connection, not authenticated at first, the client request a specific resource (like “GET /secret”). Before responding, server starts a renegotiation of the connection. This was a cause of several security failures, mostly fixed now with TLSv1. The renegotiation asks a certificate to the client for mutual authentication. Even if it is over a single TLS connection, TLS tools record two connections in the logs. The first one is not valid as it is not requesting a certificate, the second one can be valid if it requests for a certificate issued by the CAT certificate authority.

4.4 TLS Administration

4.4.1 Simulators

4.4.1.a How to create a client

Only one client is needed.

4.4.1.b How to create a server

TLS tools must provide one TLS server per protocol. Each server must be started to record connections, on a fixed port accessible from SUTs. TLS server is “dumb” as it can’t provide content to the clients tested. It acts as a proxy to a real server, using an unencrypted connection. For each protocol, an available server must be found. However, it can be simplified as follows :

- DICOM : OrderManager DICOM server
- HL7v2 : OrderManager HL7v2 server
- HTTP, Syslog, Raw : any HTTP server (Gazelle one for simplicity)

4.4.1.c How to update server parameters

Once a server it's created, we can only change its connection parameters (listening port, remote host/port).