

Introduction of ATNA - Audit Trail and Node Authentication (ATNA)

30-08-2022

Souleymane THIAM – IHE Catalyst

Summary



- Overview ATNA Profile
- Use cases
- ATNA Actors
- ATNA Transactions
- Demo in Gazelle Security Tool

Audit Trail and Node Authentication (ATNA) IHE

Profile specified by IT-Infrastructure domain (ITI)

- Status: Final Text
- Documentation:
 - <https://profiles.ihe.net/ITI/TF/Volume1/ch-9.html>
 - <https://profiles.ihe.net/ITI/TF/Volume2/ITI-19.html>
 - <https://profiles.ihe.net/ITI/TF/Volume2/ITI-20.html>

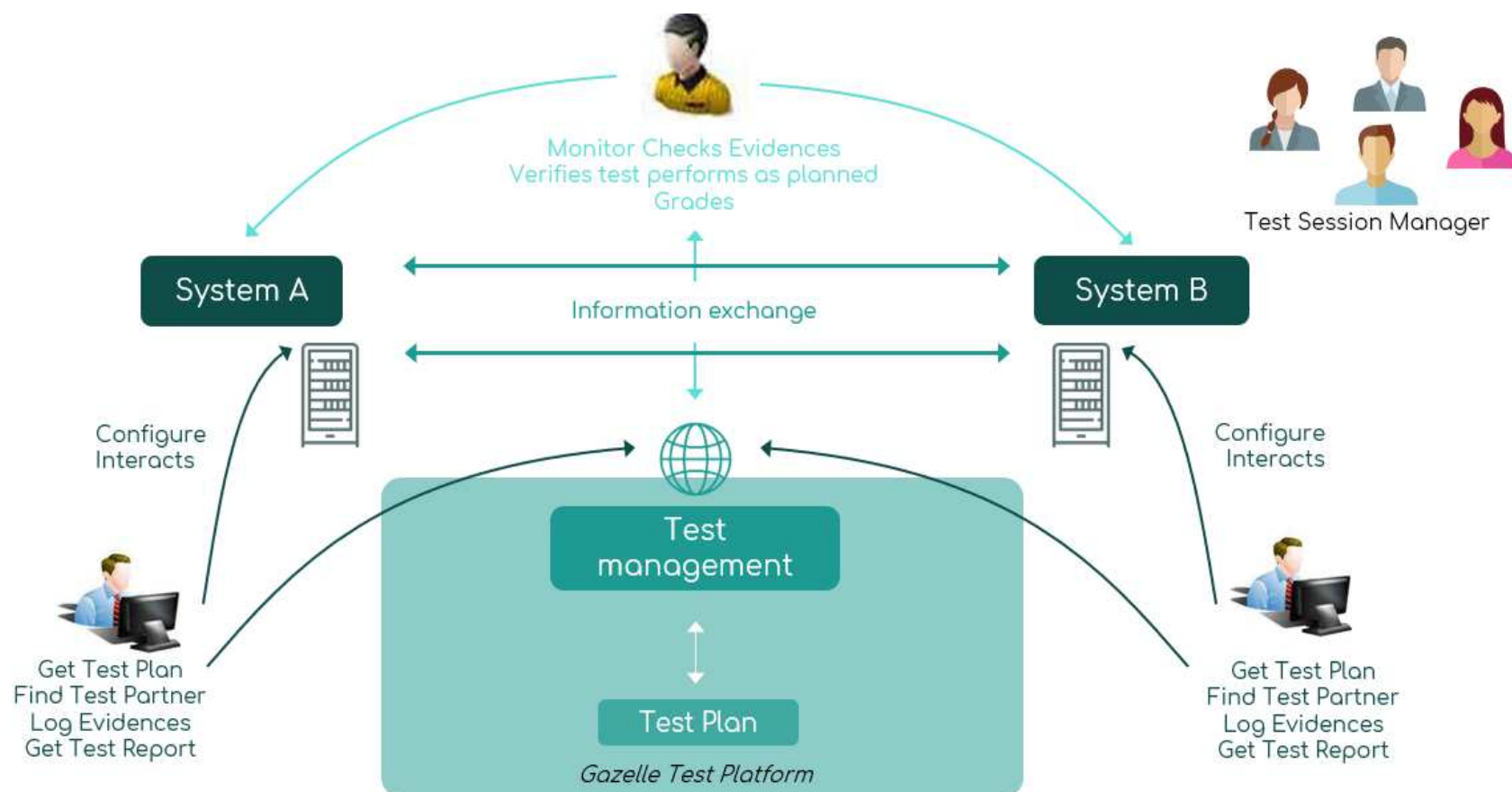
Glossary

- Audit logs: record of important events about system activity, data access or manipulation, especially patient data.
- Node: Machine on a network, either local or internet.

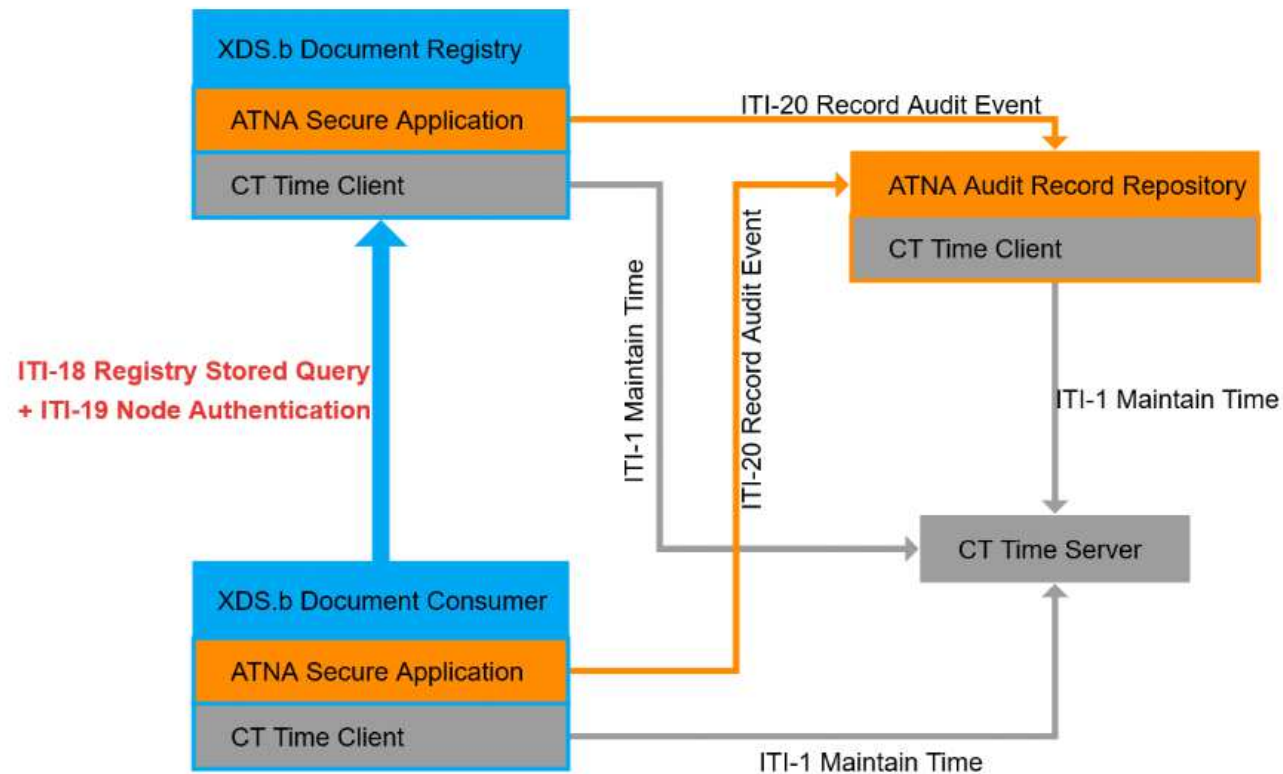
Usage

- Describe security environment (user identification, authentication, authorization and access control) for integrator to decide whether this product matches their environment.
- Defines basic auditing requirements.
- Defines communication of audit messages from secure nodes to audit record repository.
- Defines basic security requirement for network node communication.
- Defines secure application characteristics for products that are not able to meet all secure node requirements but are ready to be integrated in a secure node.
- ATNA is a cross-cutting profile, used to add a security layer on top of other IHE Profiles.

ATNA Actors and transactions : XDS.b example



ATNA Actors and transactions : XDS.b example



○ Secure Node (SN)

- Provides security and privacy (user authentication, secure communications, security audit recording and security policy enforcement) for all software and services on that system. Security considerations apply to all aspects of the system from hardware to user interface and communication devices.
- The secure node has security control over its entire stack.

The Secure Node shall

- Use Authenticate Node Transaction ITI-19 all network connections that may expose private information
- Provide authentication method to ensure for only authorized users access the Secure Node.
- Detect and report a Record Audit Event (ITI-20) for
 - All activity-related events of the SN
 - All transaction-related events of the SN
- ATNA Secure Node Actor must be grouped with CT Time Client Actor.
- System example : An ultrasound machine

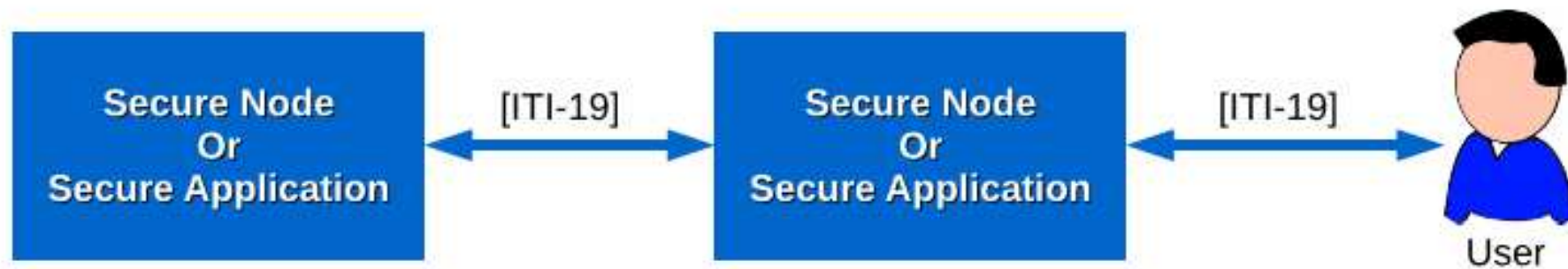
○ Secure Application (SA)

Provides security and privacy (user authentication, secure communications, security audit recording and security policy enforcement) for all actors and services grouped on that application/system. The Secure Application is not responsible for the security aspects of its environment, such as the Operating System or a database outside of its control. However, the security measures must be sufficient for the product to be ready to be integrated in a Secure Node.

The Secure Application shall

- Use Authenticate Node Transaction ITI-19 for all network connections that may expose private information
- Provide authentication method to ensure only authorized users access the Secure Application.
- Detect and report a Record Audit Event (ITI-20) for
 - All activity-related events of the SA
 - All transaction-related events of the SA
- ATNA Secure Application Actor must be grouped with CT Time Client Actor
- System example : Smartphone application

Transaction ITI-19



Transaction ITI-19



Certificate Validation

- All nodes must be authenticated (Client and Server, TLS Mutual Authentication)
- X.509 certificates based on RSA key (1024-4096) are used to authenticate the nodes
- SN/SA shall be able to perform certificate validation based either
 - on a chain of trust (CA), either
 - on a set of trusted certificates.

Access Control

- On certificate validation failure, SA/SN
 - May reject the communication, or
 - May limit access to resources appropriate for unidentified party.

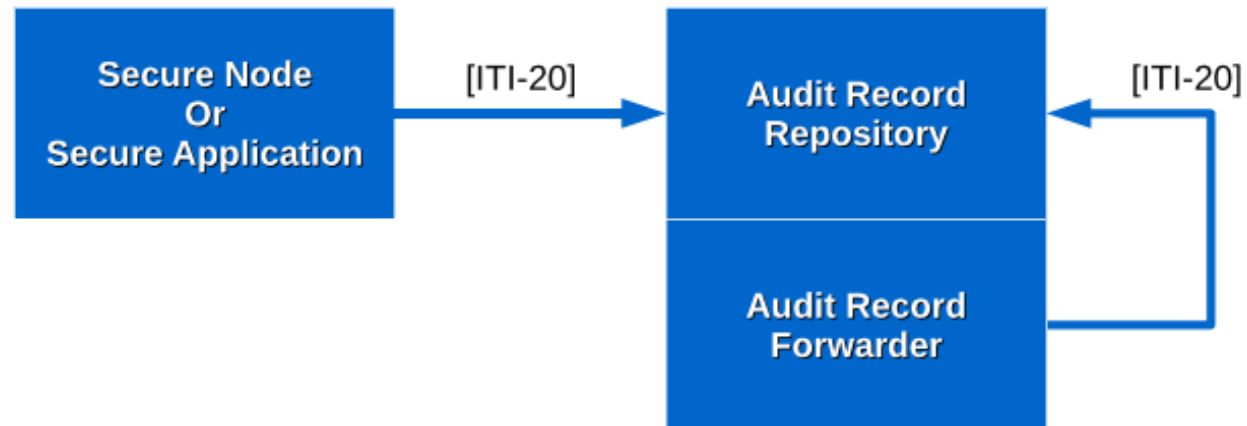
Audit Record Repository (ARR)

- Receives event audit reports and store them.
 - The Audit Record Repository shall support
 - Audit transport mechanism SYSLOG over TCP+TLS and SYSLOG over UDP as specified in ITI-20.
 - Reception of all IHE-specified audit message formats (Extensible)
 - Reception of all SYSLOG RFCs compliant audit messages. ARR may ignore or process non-IHE message formats.
 - Local security and privacy service protection and user access controls.
- ATNA Audit Record Repository Actor must be grouped with CT Time Client Actor.

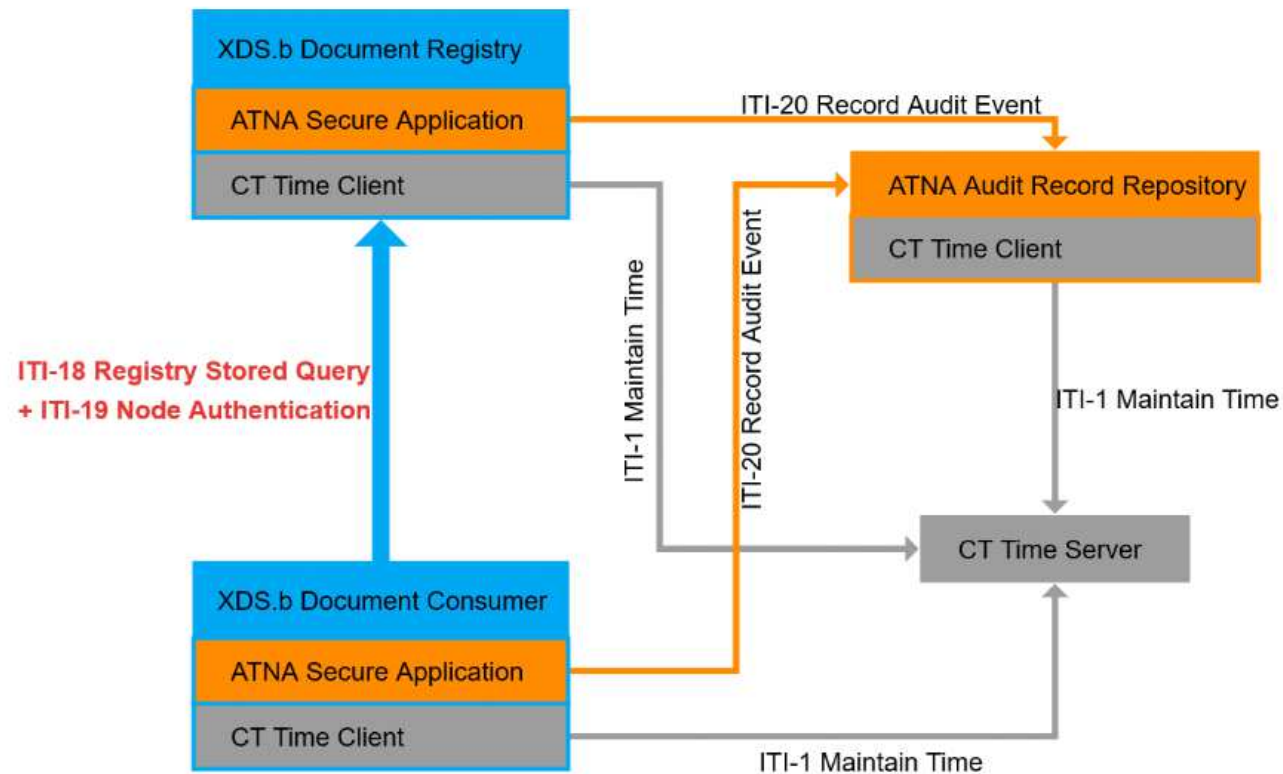
Audit Record Forwarder (ARF)

- ARF is grouped with an ARR. Upon reception of audit messages by the ARR, the ARF may filter and select some messages to forward to one or more other ARR.
- The Audit Record Forwarder shall
 - Filter and forward messages as they arrived as described in ITI-20 and Syslog RFC5424
- ATNA Audit Record Forwarder Actor must be grouped with ATNA ARR and CT Time Client Actors

Transaction ITI-20



ATNA Actors and transactions : XDS.b example



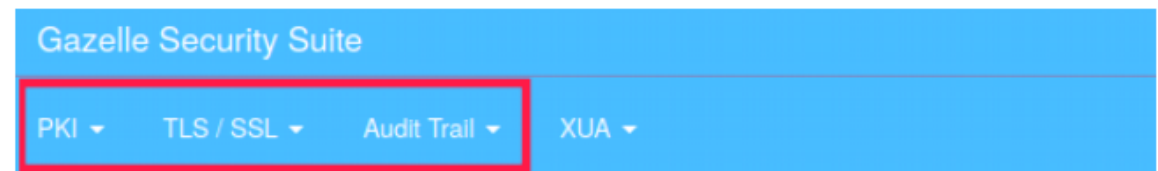
ATNA Testing

Gazelle Security Suite (GSS)



Gazelle Security Suite (GSS)

- <https://gazelle.ihe.net/gss>
- Gather Security tools of Gazelle test bed
 - PKI to get and generate certificates for testing sessions
 - TLS / SSL Simulators for SUT to verify their TLS abilities
 - Audit Message validation description (for all) and setup (for test-designers)
 - ATNA Questionnaires, for vendors to collect proof of their ATNA abilities
 - Syslog Collector, simulates a dummy ARR and verify SYSLOG Protocol.



Gazelle Security Suite

If you need to configure your firewall to receive messages Issued by Gazelle Security Suite, the I

LATEST

- 2019-09-26: **Please read this [ATNA Testing Information Page](#)** if you will be testing at an
- 2017-11-15 : ATNA Questionnaires can be updated if the system registration changes in G
- 2017-09-06 : TLSv1.2 is now supported

OVERVIEW

This tool is used for several ATNA-profile-related functions for Connectathons:

GSS PKI



Gazelle Security Suite, PKI

- Request a certificate
 - With CSR or
 - Without (key pair is generated by GSS)
- List pending certificate requests
 - Can be accepted by administrator, or
 - Automatically accepted
- List existing certificates
 - List all certificates that have been generated by GSS
- Testing Certificate Authority is usually given on GSS home page, ask the Testing Session Manager if not

The screenshot shows the 'Gazelle Security Suite' interface. The 'PKI' menu is highlighted with a red circle. The dropdown menu includes: 'Request a certificate', 'List certificate requests', 'List certificates', 'Install browser certificate for CAS auto-login', and 'Certificate validation'. Red arrows point from the text in the list to these menu items. Below the menu is a 'LATEST' section with news items. One item is circled in red: 'The CA certificate is available [here](#).' Below this is a section titled 'TEST YOUR TLS IMPLEMENTATION:' with a list of TLS server simulators.

Gazelle Security Suite

PKI ▼ TLS / SSL ▼ Audit Trail ▼ XUA ▼

- Request a certificate
- List certificate requests
- List certificates
- Install browser certificate for CAS auto-login
- ✓ Certificate validation

messages issued by Gazelle Security Suite

LATEST

- Please read this [ATNA Testing Information Page](#) if you will be testing at an IHE N
- 2017-11-15 : ATNA Questionnaires can be updated if the system registration chang

ATNA promise

- The ATNA questionnaire.

DIGITAL CERTIFICATES for Conformity Assessment Testing :

The CA certificate is available [here](#).

TEST YOUR TLS IMPLEMENTATION:

- **TLS SERVER SIMULATORS:** To check your SUT as a **consumer/client**, the tool will act as a server. Yo
 - [HL7 V2 server](#) (<domain_or_IP>:20007)
 - [HTTPS server](#) (<domain_or_IP>:20011)
 - [Syslog server](#) (<domain_or_IP>:20009)
 - ["Amu" server](#) (<domain_or_IP>:20070)

GSS ATNA Questionnaire



Gazelle Security Suite, ATNA Questionnaire
Questionnaires available in Audit Trail menu
List all questionnaires

- Of your organization if vendor
- Any questionnaire if monitor/admin
- Questionnaires can be
 - Created (owner)
 - Viewed (owner, monitor and admin)
 - Edited (owner and admin)
 - Reviewed (monitor and admin)
 - Deleted (owner and admin)

The screenshot displays the Gazelle Security Suite interface. The top navigation bar includes 'PKI', 'TLS / SSL', 'Audit Trail', and 'JA'. The 'Audit Trail' menu is highlighted with a red circle, and its dropdown menu is open, showing 'Audit message specifications', 'ATNA Questionnaires' (highlighted with a red arrow), and 'Syslog Collector'. Below the navigation bar, the 'ATNA Questionnaires' section is visible, featuring a '+ New ATNA Questionnaire' button (highlighted with a red box) and an 'Edit ATNA Questionnaire template' button. A search criteria section allows filtering by 'Testing session', 'Institution', 'System', 'Status', 'Creator', 'Reviewer', and 'Last modified on'. Below the search criteria is a table of questionnaires:

System's keyword	Testing session	Status	Owner	Last modifier	Last modified on	Action
OTHER_GE_CCA_CAS2019	CAS-2-2019-TS1	Reviewed and not valid	dsuabramanian (CATS)	cecoche (CATS)	2/28/19 4:05:53 PM (CET GMT+0100)	[Icons]
OTHER_GE_CEA	CAS-2-2019-TS2	Reviewed and valid	incatella (CATS)	cecoche (CATS)	10/16/19 5:36:31 PM (CEST GMT+0200)	[Icons]
TEMPLATE	Demonstration	In Progress	aberge (null)	aberge (null)	4/2/15 8:25:03 PM (CEST GMT+0200)	[Icons]

At the bottom, there is a 'Number of results per page' dropdown set to 20. The 'Action' column for the 'TEMPLATE' row is highlighted with a red circle.

GSS ATNA Questionnaire



ATNA Questionnaire

Questionnaires contain meta information on the system

Questionnaires for SA have 5 tabs

- Inbound and outbound communications (2 tabs)
- Local authentication
- Audit Messages
- TLS Tests

Questionnaires for SN have a 6th tab

- To describe others protections of the node

The screenshot displays the GSS ATNA Questionnaire interface. It is divided into two main panels: "System details" on the left and "Questionnaire details" on the right. The "System details" panel contains fields for "System's keyword" (ARR_IHE-EU_Syslog_Collector_COPY_0), "System's organization" (IHE-EU), "Testing session" (Dummy Session for Gazelle Testing Purposes), and "System type" (Secure Node (SN)), which is circled in red. The "Questionnaire details" panel shows "Questionnaire's status" (Ready for review), "Permanent link" (https://gazelle.ihe.net/gss/questionnaire/viewer.seam?id=276), "Creator" (ceoche (EU)), "Last modifier" (ceoche (EU)), and "Last modified on" (2/22/21 3:39:16 PM (CET GMT+0100)). Below these panels is a "Back to list" button and a green checkmark icon with the text "The ATNA Questionnaire is up to date with Gazelle TM registration", which is also circled in red. At the bottom, there is a horizontal navigation bar with tabs: "Inbound network communications", "Outbound network communications" (selected), "Authentication process for local users", "Audit messages", "Non network means for accessing PHI", and "TLS tests".

System details	
System's keyword	ARR_IHE-EU_Syslog_Collector_COPY_0
System's organization	IHE-EU
Testing session	Dummy Session for Gazelle Testing Purposes
System type	Secure Node (SN)

Questionnaire details	
Questionnaire's status	Ready for review
Permanent link	https://gazelle.ihe.net/gss/questionnaire/viewer.seam?id=276
Creator	ceoche (EU)
Last modifier	ceoche (EU)
Last modified on	2/22/21 3:39:16 PM (CET GMT+0100)

Back to list ✓ The ATNA Questionnaire is up to date with Gazelle TM registration

Inbound network communications | Outbound network communications | Authentication process for local users | Audit messages | Non network means for accessing PHI | TLS tests

GSS ATNA Questionnaire



ATNA Questionnaire, Audit Message tab

Differentiate implemented/non-implemented Audit Messages.

Sample should be uploaded and GSS will run the validation and compute the status

Audited Event ▲	Audited transaction ▼	Issuing actor ▼	Implemented ?	Sample file	Comment	Validation status ▼
Application-activity (start)	NULL - NULL	Secure Application	no	10400_APP_START.xml	Validator: 1.3.6.1.4.1.12559.11.1.2.1.12.64 Not Implemented	Passed
Application-activity (stop)	NULL - NULL	Secure Application	no	10399_APP_STOP.xml	Validator: 1.3.6.1.4.1.12559.11.1.2.1.12.65 Not Implemented	Passed
Patient-record-event	ITI-10 - PIX Update Notification	Patient Identifier Cross-reference Consumer	yes	10401_ITI_10_PIC.xml	Validator: 1.3.6.1.4.1.12559.11.1.2.1.12.85	Passed
Patient-record-event	ITI-10 - PIX Update Notification	Patient Identity Cross-reference Manager	no		Validator: 1.3.6.1.4.1.12559.11.1.2.1.12.86 I dropped the actor for this Event from my registration	No file uploaded
Patient-record-event (Admit/Register or Update Patient)	ITI-8 - Patient Identity Feed	Patient Identity Cross-reference Manager	no		Validator: 1.3.6.1.4.1.12559.11.1.2.1.12.15 I dropped the actor for this Event from my registration	No file uploaded
Patient-record-event (Admit/Register or Update Patient)	ITI-8 - Patient Identity Feed	Patient Identity Source	yes	10404_ITI_8_PIS.xml	Validator: 1.3.6.1.4.1.12559.11.1.2.1.12.13	Passed

GSS ATNA Questionnaire



ATNA Questionnaire, TLS tab

Test at least on TLS connection per outbound/inbound type (Syslog, HL7v2, HTTP, DICOM or Raw)

TLS Simulator links must copy in this tab, status is computed

✓ The TLS Tests list is up to date

Search Criteria				
Tested side	Show all	×	Status	Show all
Connection type	Show all	×		
Tested side ▲	Connection type ▲	Test URL	Comment	Status ▲
CLIENT	Raw	https://gazelle.ihe.net/gss/details/connection.seam?id=4143313		Passed
CLIENT	HL7v2	https://gazelle.ihe.net/gss/details/connection.seam?id=4143306		Passed
CLIENT	Syslog	https://gazelle.ihe.net/gss/details/connection.seam?id=4143282		Passed
SERVER	HL7v2	https://gazelle.ihe.net/gss/details/connection.seam?id=4143179		Passed
SERVER	Raw	https://gazelle.ihe.net/gss/details/connection.seam?id=4143209		Passed

GSS TLS Simulators



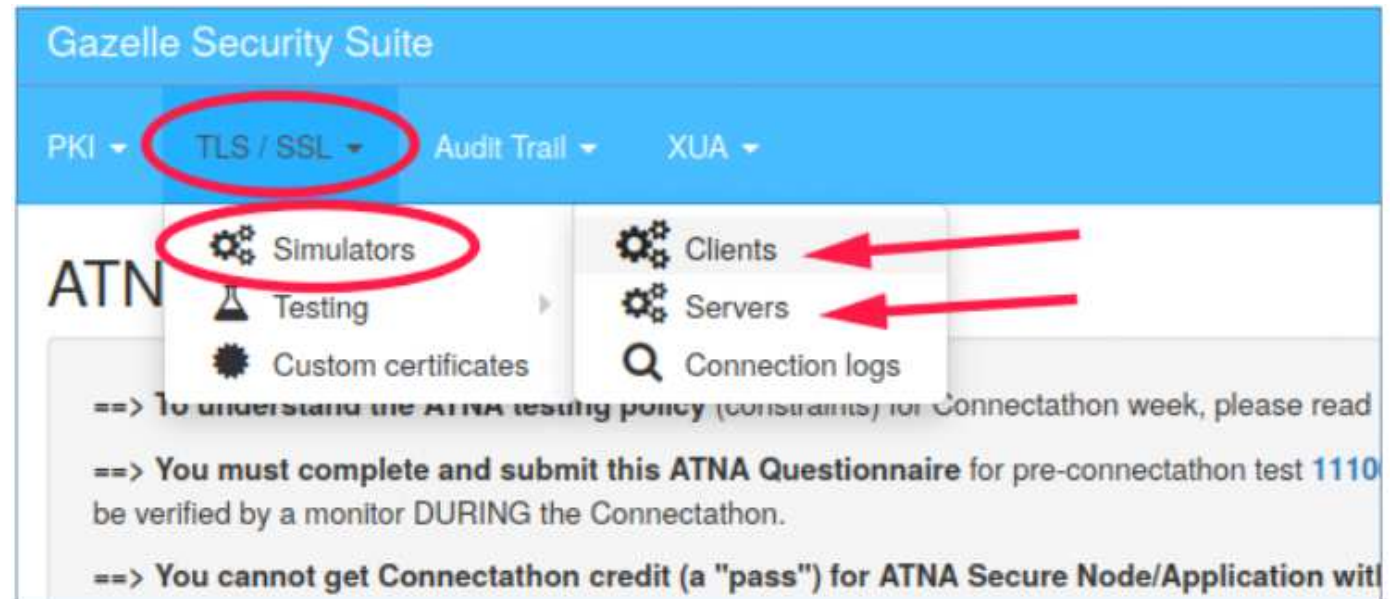
Gazelle Security Suite, TLS Simulators

TLS Simulators Client

- To test SUT Servers

TLS Simulators Servers

- To test SUT Clients



GSS TLS Simulators



TLS/SSL client simulator

TLS Parameters of the Client Simu

Simulator identity	
Keyword	Test TLS Client
Certificate	C=FR,O=IHE Europe,CN=Gazelle Simulators
Peer authentication	
Trusted issuers	C=FR,O=IHE-EUROPE-CATS,CN=conformity-assessment-testing.ihe-europe.net,GIVENNAME=Eric,SERIALNUMBER=Poiseau,OU=IHE Services,E=eric.poiseau@inria.fr
Certificate validator	TLS server
Check revocation	false
Security parameters	
Supported protocols	TLSv1
Supported cipher suites	TLS_RSA_WITH_AES_128_CBC_SHA

[Back to list](#)

Start connection	
Client type *	RAW
Message *	Hello
Target host *	
Target port *	1
Start client	

Form to trigger a TLS Connection with a Server

Logs below those panels

GSS TLS Simulators



TLS/SSL server simulator

Simulator identity	
Keyword	Test HTTPS/WS Server
Certificate	C=FR,O=IHE Europe,CN=TLS Testing Server

Peer authentication	
Client authentication	Required
Trusted issuers	C=FR,O=IHE-EUROPE-CATS,CN=conformity-assessment-testing.ihe-europe.net,GIVENNAME=Eric,SERIALNUMBER=Poiseau,OU=IHE Services,E=eric.poiseau@lnria.fr
Certificate validator	TLS client
Check revocation	false

Security parameters	
Supported protocols	TLSv1
Supported cipher suites	TLS_RSA_WITH_AES_128_CBC_SHA

[Back to list](#)

Network parameters	
Status	Running
Server type	HTTP
Server IP/Host	51.83.86.147 (51.83.86.147)
Server port	20011
Forward to	localhost:80

[Edit parameters](#) [Stop server](#)

Server simulators are listening incoming connections on this host:port

GSS TLS Simulators



TLS/SSL connection

Connection details

Permanent link: <https://ihe-conformity-assessment.koreval.com/gss/details/connection.seam?id=202>

Connection date: 8/1/19 10:58:40 AM (CEST GMT+0200)

SUT address: 68.93.142.84 lightspeed.rhinc.sbcglobal.net:8443

SUT certificates:

- C=US,O=GE,CN=68.93.142.84,T=Mr.GIVENNAME=Malcolm,SURNAME=Catella,OU=EA

Simulator address: 51.83.86.147:41850

Simulator keyword: Test TLS Client test

Simulator certificate: C=FR,O=IHE Europe,CN=TLS Testing Client

Handshake success

Protocol: TLSv1

Cipher suite: TLS_RSA_WITH_AES_128_CBC_SHA

Warning message: Server asked for a certificate, but list of certificate authorities in the server response is empty. Some client may refuse such TLS handshake (see RFC2246 section 7.4.4)

TLS/SSL events

Date: 08/01/2019 08:58:40.670

Type: CHECK_TRUSTED_SERVER

Details:

result=PASSED

- C=US,O=GE,CN=68.93.142.84,T=Mr.GIVENNAME=Malcolm,SURNAME=Catella,OU=EA

Date: 08/01/2019 08:58:40.671

Type: CHOOSE_ALIAS_CLIENT

Details:

Key types:

- RSA
- DSA
- EC

Details

Key types:

- RSA
- DSA
- EC

Issuers:

Intercepted messages

Connection Id	Index	Type	Details	Date	Time (µs)	From	To	Proxy	Info
493	2			8/1/19 10:58:41 AM (CEST GMT+0200)	682836	127.0.0.1 : 52266	68.93.142.84 : 8443	1024	
493	1			8/1/19 10:58:40 AM (CEST GMT+0200)	573338	127.0.0.1 : 52266	68.93.142.84 : 8443	1024	application/soap+xml

Number of results per page: 20

GSS TLS Simulators



TLS/SSL connection

Connection details

Permanent link

Connection date

SUT address

SUT certificates

Simulator address

Simulator keyword

Simulator certificate

Handshake success

Protocol

Cipher suite

Warning message

https://ihe-conformity-assessment.koreval.com/gss/details/connection.seam?id=202

8/1/19 10:58:40 AM (CEST GMT+0200)

68.93.142.84 lightspeed.rhinc.sbcglobal.net:8443

- C=US,O=GE,CN=68.93.142.84,T=Mr.GIVENNAME=Malcolm,SURNAME=Catella,OU=EA

51.83.86.147:41850

Test TLS Client test

C=FR,O=IHE Europe,CN=TLS Testing Client

SSLV1

TLS_RSA_WITH_AES_128_CBC_SHA

Server asked for a certificate, but list of certificate authorities in the server response is empty. Some client may refuse such TLS handshake (see RFC2246 section 7.4.4)

TLS/SSL events

Date

Type

Details

08/01/2019 08:58:40.670

CHECK_TRUSTED_SERVER

Details

result=PASSED

- C=US,O=GE,CN=68.93.142.84,T=Mr.GIVENNAME=Malcolm,SURNAME=Catella,OU=EA

Date

Type

Details

08/01/2019 08:58:40.671

CHOOSE_ALIAS_CLIENT

Key types :

- RSA
- DSA
- EC

Details

Key types :

- RSA
- DSA
- EC

Issuers :

Intercepted messages

Connection Id	Index	Type	Details	Date	Time (µs)	From	To	Proxy	Info
493	2	←	Details	8/1/19 10:58:41 AM (CEST GMT+0200)	682836	127.0.0.1 : 52266	68.93.142.84 : 8443	1024	
493	1	→	Details	8/1/19 10:58:40 AM (CEST GMT+0200)	573338	127.0.0.1 : 52266	68.93.142.84 : 8443	1024	application/soap+xml

Number of results per page : 20

RACSEL
RESEAU ASSOCIÉ DES CENTRES DE RECHERCHE EN SANTÉ
MÉDICALLE ET SOCIALE

REGIONAL
PUBLIC GOODS
Région de Bruxelles-Capitale

BID
Bureau International de Développement

2
4

An abstract graphic on the left side of the slide, consisting of several overlapping circles and organic shapes in various shades of red and maroon, resembling a molecular structure or a network diagram.

Questions ?