QHIN Conformance Testing Process: Security Test Cases

For Candidate QHIN Conformance Testing

Version History

Version	Description of Change	Version Date
1.0	Initial Publication	September 9, 2022
1.0.1	Removed 14 Test Cases that did not align with the QHIN Technical Framework (QTF) requirements; updated language clarifying SAML assertion testing details and data load set/test patient requirements; and aligned language with the TEFCA Standard Operating Procedures (SOPs).	December 6, 2022
1.0.2	Remove one Test Case related to timestamp signature.	February 6, 2023
1.0.3	Updated Title to include "For Candidate QHIN Conformance Testing" only.	May 31, 2203

1 QHIN Conformance Testing Process Overview ... 4

2 Security Test Case List ... 5

3 Tests for Initiating QHIN Candidate ... 6

4 Tests for Responding QHIN Candidate ... 6

TC: MAPD-R-0003.000 Handle missing wsse:Security element ... 6

TC:MAPD-R-0003.201 Handle missing MessageID element ... 7

TC:MAPD-R-0003.301 Handle missing assertion signature element ... 9

TC:MAPD-R-0003.302 Handle invalid assertion signature ... 11

TC: MAPD-R-0003.326 Handle missing KeyInfo in assertion signature ... 13

TC:MAPD-R-0003.401 Handle missing Assertion element ... 15

TC:MAPD-R-0003.402 Handle an invalid Version in the Assertion ... 17

TC:MAPD-R-0003.403 Handle missing Version in Assertion element ... 19

TC:MAPD-R-0003.407 Handle invalid IssueInstant in Assertion element ... 21

TC:MAPD-R-0003.408 Handle IssueInstant much later than Message Timestamp ... 23

TC:MAPD-R-0003.409 Handle missing Issuer in Assertion element ... 25

TC:MAPD-R-0003.410 Handle missing Issuer Format in Assertion ... 27

TC:MAPD-R-0003.411 Handle invalid Issuer Email Name ID in Assertion ... 29

TC:MAPD-R-0003.412 Handle invalid Issuer X.509 Name ID in Assertion ... 31

TC: MAPD-R-0003.413 Handle invalid Issuer Windows Name ID in Assertion ... 33

TC: MAPD-R-0003.420 Handle missing Subject element in Assertion ... 35

TC: MAPD-R-0003.421 Handle missing Subject NameID in Assertion ... 37

TC: MAPD-R-0003.422 Handle invalid Subject NameID in Assertion ... 39

TC: MAPD-R-0003.423 Handle missing Subject Confirmation in Assertion ... 41

TC: MAPD-R-0003.424 Handle missing Subject Confirmation Method in Assertion ... 43

1 QHIN Conformance Testing Process Overview

The scope of the Recognized Coordinating Entity (RCE)/QHIN Testing Process is limited to the Qualified Health Information Network (QHIN) Technical Framework (QTF) Version 1, the information outlined in the Common Agreement, and related QHIN Testing Process document(s).

Changes to the QHIN Testing Process documents may be updated in accordance with the QTF, which may be updated in accordance with changes to industry standards and specifications.

The scope of the QHIN Testing Process document(s) supports the following:

- Prospective QHINs in the Conformance Testing Process;
- QHINs who wish to test new technology or retest as a condition of continued participation in the Common Agreement; and
- Vendors who wish to have their product(s) validated as QHIN compliant. The Conformance Testing Process verifies that a system both complies with the QTF specifications and has the ability to interoperate with other QHINs.

The abbreviation of System Under Test (SUT) will be used to describe the role of the testing organization in the following test cases. The summary of security test cases can be found below:

Table 1: Security Test Summary

SUT	Description	Specifications	Summary of Test Cases	Test Method
QHIN	Transmitting clinical documentation to support treatment of an individual, care coordination, or transitions of care	QHIN Technical Framework (QTF) Version 1	20 required security tests	Run tests against the Sequoia Interoperability Testing Platform (ITP) Results validated by the Sequoia Project

These test cases are currently in effect and are required for organizations wishing to complete Pre-Production. These materials reflect the following:

- QHIN Testing Overview - A broad overview of the process, applications, and documentation for the Conformance Testing Process. List of all QHIN test cases, documentation, conformity assessment checklists, and a description of content tests for the Conformance Testing Process.
- Test Data Load Set – Required data and associated document files to execute the test cases within the Sequoia Interoperability Testing Platform (ITP) including patient demographics, sample documents, as well as the mapping of the documents to the individuals. The demographic data must be loaded into the SUT exactly as prescribed in the patients.csv spreadsheet and all attributes must be loaded (unless the attribute is an optional element and it is not supported by the SUT). CCDA files and other clinical data included in the Test Data Load Set are provided as examples.

2 Security Test Case List

The following table lists the security tests that must be completed for the Conformance Testing Process. The following list of 21 test cases are required to pass the Security component of testing for Pre-Production Testing.

The security test cases currently require no specific preloading of data and/or associated document files as only SOAP security, XML security, and SAML assertion elements are in scope.

TABLE 2: SECURITY TEST CASE LIST

#	TEST CASE ID	FUNCTIONAL AREA	PURPOSE/ DESCRIPTION
1	TC-MAPD-R-0003.000	SOAP security	Handle missing wsse:Security element
2	TC-MAPD-R-0003.201	WS-Addressing	Handle missing MessageID element
3	TC-MAPD-R-0003.301	XML Signature	Handle missing Assertion signature element
4	TC-MAPD-R-0003.302	XML Signature	Handle invalid Assertion signature
5	TC-MAPD-R-0003.326	XML Signature	Handle Missing KeyInfo in Assertion signature
6	TC-MAPD-R-0003.401	SAML Assertion	Handle missing Assertion element
7	TC:MAPD-R-0003.402	SAML Assertion	Handle an invalid Version in the Assertion
8	TC:MAPD-R-0003.403	SAML Assertion	Handle missing Version in Assertion element
9	TC:MAPD-R-0003.407	SAML Assertion	Handle invalid IssueInstant in Assertion element
10	TC:MAPD-R-0003.408	SAML Assertion	Handle IssueInstant much later than Message Timestamp
11	TC:MAPD-R-0003.409	SAML Assertion	Handle missing Issuer in Assertion element
12	TC-MAPD-R-0003.410	SAML Assertion	Handle Missing Issuer Format in Assertion
13	TC-MAPD-R-0003.411	SAML Assertion	Handle Invalid Issuer Email Name ID in Assertion
14	TC-MAPD-R-0003.412	SAML Assertion	Handle Invalid Issuer X.509 Name ID in Assertion

#	TEST CASE ID	FUNCTIONAL AREA	PURPOSE/ DESCRIPTION
15	TC-MAPD-R-0003.413	SAML Assertion	Handle Invalid Issuer Windows Name ID in Assertion
16	TC-MAPD-R-0003.420	SAML Assertion	Handle Missing Subject element in Assertion
17	TC-MAPD-R-0003.421	SAML Assertion	Handle Missing Subject Name ID in Assertion
18	TC-MAPD-R-0003.422	SAML Assertion	Handle Invalid Subject Name ID in Assertion
19	TC-MAPD-R-0003.423	SAML Assertion	Handle Missing Subject Confirmation in Assertion
20	TC-MAPD-R-0003.424	SAML Assertion	Handle Missing Subject Confirmation Method in Assertion

3 TESTS FOR INITIATING QHIN CANDIDATE

The RCE/QHIN Testing Process for Qualified Health Information Network (QHIN) Technical Framework (QTF) Version 1 Specification does not currently specify negative tests for Initiating QHIN candidates.

4 TESTS FOR RESPONDING QHIN CANDIDATE

TC: MAPD-R-0003.000 Handle missing wsse:Security element

Test Case ID:	**TC: MAPD-R-0003.000**
Title:	Handle missing wsse:Security element
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing wsse:Security element.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header missing the Security element.
2. The System returns either
   a. SOAP fault to the Testing Tool with text describing the relevant error, or
   b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC:MAPD-R-0003.201 Handle missing MessageID element

Test Case ID:	TC: MAPD-R-0003.201
Title:	Handle missing MessageID element
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing MessageID element.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header missing MessageID.
2. The System returns either
   a. SOAP fault to the Testing Tool with text describing the relevant error, or
   b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC:MAPD-R-0003.301 Handle missing assertion signature element

Test Case ID:	**TC: MAPD-R-0003.301**
Title:	Handle missing assertion signature element
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing Security/Assertion/Signature element.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SAML assertion missing Security/Assertion/Signature.
2. The System returns either
   a. SOAP fault to the Testing Tool with text describing the relevant error, or
   b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC:MAPD-R-0003.302 Handle invalid assertion signature

Test Case ID:	**TC: MAPD-R-0003.302**
Title:	Handle invalid assertion signature
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with an invalid Security/Assertion/Signature.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with an invalid SAML assertion Signature.
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC: MAPD-R-0003.326 Handle missing KeyInfo in assertion signature

Test Case ID:	**TC: MAPD-R-0003.326**
Title:	Handle missing KeyInfo in assertion signature
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing KeyInfo in assertion signature.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/Signature/KeyInfo missing
2. The System returns either
   a. SOAP fault to the Testing Tool with text describing the relevant error, or
   b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC:MAPD-R-0003.401 Handle missing Assertion element

Test Case ID:	**TC: MAPD-R-0003.401**
Title:	Handle missing Assertion element
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing Assertion element.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion missing
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC:MAPD-R-0003.402 Handle an invalid Version in the Assertion

Test Case ID:	**TC: MAPD-R-0003.402**
Title:	Handle an invalid Version in the Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with an invalid version in the Assertion element.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/@Version is not "2.0"
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
December 6, 2022	Initial Draft Version

TC:MAPD-R-0003.403 Handle missing Version in Assertion element

Test Case ID:	**TC: MAPD-R-0003.403**
Title:	Handle invalid missing Version in Assertion element
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing Version in the Assertion element.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/@Version missing.
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
December 6, 2022	Initial Draft Version

TC:MAPD-R-0003.407 Handle invalid IssueInstant in Assertion element

Test Case ID:	**TC: MAPD-R-0003.407**
Title:	Handle invalid IssueInstant in Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with an invalid IssueInstant in the Assertion element.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/@IssueInstant is not a valid xs:DateTime as described in https://www.w3.org/TR/xmlschema-2/
2. The System returns either
   a. SOAP fault to the Testing Tool with text describing the relevant error, or
   b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
December 6, 2022	Initial Draft Version

TC:MAPD-R-0003.408 Handle IssueInstant much later than Message Timestamp

Test Case ID:	**TC: MAPD-R-0003.408**
Title:	Handle IssueInstant in Assertion much later than Message Timestamp
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with an IssueInstant in the Assertion element that is much later than the Message Timestamp

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/@IssueInstant 24 hours after the Message Time Stamp Created value.
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
December 6, 2022	Initial Draft Version

TC:MAPD-R-0003.409 Handle missing Issuer in Assertion element

Test Case ID:	**TC: MAPD-R-0003.409**
Title:	Handle missing Issuer in Assertion element
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing Issuer in the Assertion element.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/@IssueInstant missing
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
December 6, 2022	Initial Draft Version

TC:MAPD-R-0003.410 Handle missing Issuer Format in Assertion

Test Case ID:	**TC: MAPD-R-0003.410**
Title:	Handle missing Issuer Format in Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing Issuer Format in Assertion.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/Issuer/@Format missing.
2. The System returns either
   a. SOAP fault to the Testing Tool with text describing the relevant error, or
   b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC:MAPD-R-0003.411 Handle invalid Issuer Email Name ID in Assertion

Test Case ID:	**TC: MAPD-R-0003.411**
Title:	Handle invalid Issuer Email Name ID in Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing Issuer Email Name ID in Assertion.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/Issuer/@Format = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" but the value supplied is not a valid email address format
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC:MAPD-R-0003.412 Handle invalid Issuer X.509 Name ID in Assertion

Test Case ID:	**TC: MAPD-R-0003.412**
Title:	Handle invalid Issuer X.509 Name ID in Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with an invalidIssuer X.509 Name ID in Assertion.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/Issuer/@Format = "urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName" but the value supplied is not a valid X.509 Subject Name format
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC: MAPD-R-0003.413 Handle invalid Issuer Windows Name ID in Assertion

Test Case ID:	**TC: MAPD-R-0003.413**
Title:	Handle invalid Issuer Windows Name ID in Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with an invalidWindows Name ID in Assertion.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/Issuer/@Format = "urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName" but the value supplied is not a valid Window Domain Qualified Name format
2. The System returns either
   a. SOAP fault to the Testing Tool with text describing the relevant error, or
   b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC: MAPD-R-0003.420 Handle missing Subject element in Assertion

Test Case ID:	**TC: MAPD-R-0003.420**
Title:	Handle missing Subject element in Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing Subject element in Assertion.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/Subject missing
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	**Changes**
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC: MAPD-R-0003.421 Handle missing Subject NameID in Assertion

Test Case ID:	**TC: MAPD-R-0003.421**
Title:	Handle missing Subject NameID in Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing Subject NameID element in Assertion.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/ Assertion/Subject/NameID missing
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC: MAPD-R-0003.422 Handle invalid Subject NameID in Assertion

Test Case ID:	**TC: MAPD-R-0003.422**
Title:	Handle invalid Subject NameID in Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with an invalid Subject NameID in Assertion.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/Subject/NameID/@Format is invalid
2. The System returns either
   a. SOAP fault to the Testing Tool with text describing the relevant error, or
   b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC: MAPD-R-0003.423 Handle missing Subject Confirmation in Assertion

Test Case ID:	**TC: MAPD-R-0003.423**
Title:	Handle missing Subject Confirmation in Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing Subject Confirmation element in Assertion.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/Subject/SubjectConfirmation missing
2. The System returns either
   a. SOAP fault to the Testing Tool with text describing the relevant error, or
   b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	Changes
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.

TC: MAPD-R-0003.424 Handle missing Subject Confirmation Method in Assertion

Test Case ID:	**TC: MAPD-R-0003.424**
Title:	Handle missing Subject Confirmation Method in Assertion
SUT Role:	Responding Gateway
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple Patient Discovery (PD) Request to the System with a missing Subject Confirmation Method element in Assertion.

Preconditions

Data Load Set: N/A

Test Case Patient Association: N/A

Test Steps

1. The Testing Tool sends a synchronous Patient Discovery Request to the System with the SOAP header element Security/Assertion/Subject/SubjectConfirmation/@Method is missing
2. The System returns either
    a. SOAP fault to the Testing Tool with text describing the relevant error, or
    b. a normal response, but without performing the requested action due to local security policy. For example, a normal response is returned with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Referenced Specifications

Secure Use of Transport Layer Security (TLS)	*The Transport Layer Security (TLS) Protocol Version 1.2* (IETF RFC 5246) - available at: https://tools.ietf.org/html/rfc5246 and *The Transport Layer Security (TLS) Protocol Version 1.3* (IETF RFC 8446) – available at https://tools.ietf.org/html/rfc8446
Security Assertion Markup Language (SAML)	*Security Assertion Markup Language* (SAML) – available at: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
IHE Cross-Enterprise User Assertion (XUA)	*IHE Cross-Enterprise User Assertion (XUA) profile* - available in the IHE IT Infrastructure (ITI) Technical Framework Volume 1: Integration Profiles at: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Rev17-0_Vol1_FT_2020-07-20.pdf

Change History

Date	**Changes**
April 1, 2022	Initial Draft Version
December 6, 2022	Updated language clarifying SAML assertion details and data load set/test patient requirements.