2011

eHealth Exchange Required Testing Security Package (Participant & Product Testing)

2011 Security Testing

Required

(Participant & Product)

Table of Contents

General Notes for Required Security Testing for Participant and Product Programs

The scope of the eHealth Exchange Testing Program is limited to the Specifications; the information outlined in the Validation Plan and related Test Materials adopted by the Coordinating Committee, collectively called "Performance and Service Specifications".

Testing requirements may vary depending upon Specification version(s), as well as the profiles (i.e. use cases) that an Applicant or Participant wishes to support. The summary of test cases related to the Smoke Tests can be found below.

Changes to the profiles, Specifications, Validation Plan and Test Materials may be made in accordance with the applicable change processes described in the DURSA.

Profile	Description	Specifications	Summary of Test Cases	Test Method
Treatment Authorized Release of Information (SSA)	Transmitting clinical documentation to support treatment of an individual, care coordination or transitions of care Transmit clinical documentation to the Social Security Administration (SSA) for the purposes of supporting a claimant's eligibility for Social Security disability benefits	2010 version of the following • Messaging Platform • Authorization Framework • Patient Discovery • Query for Documents • Retrieve Documents	• Smoke tests (2010)	Run tests against Developers Integration Lab (DIL) Testing environment Results validated by the Sequoia Project
		2011 version of the following • Messaging Platform • Authorization Framework • Patient Discovery • Query for Documents • Retrieve Documents	• Smoke tests (2011) • Security interoperability tests (2011)	Run tests against Developers Integration Lab (DIL) Testing environment Results validated by the Sequoia Project
		At least one of the following clinical document types • Basic C32 • Bridge C32 • HL7 C-CDA v1.1 US Realm	Set up test data Generate sample Message	Run sample Message through the corresponding NIST validator tool Results validated by the Sequoia Project

eHealth Exchange Specifications

2010 eHealth Exchange Specifications

These initial production specifications are in limited use and the participants currently using the 2010 specification are migrating to support 2011 specifications in preparation for their future sunset. The sunset date is yet to be determined. Organizations using a previously validated System under the prior onboarding program have the option of only conducting the below tests:

- 6 smoke interoperability tests (2010)

2011 eHealth Exchange Specifications

These production specifications are currently in effect and are required for organizations that are not using a previously validated System under the prior onboarding program and use a System supporting the 2011 specifications.

- 6 smoke interoperability tests (2011)
- 35 Required Security tests
    - The Security Test Cases on the following page only focus on Messaging Platform and Authorization Framework (MA), but do not validate PD/QD/RD beyond the Smoke Test cases, which validate the responder only role.
    - These MA Required Security Tests are only applicable to the 2011 Edition Testing for applicable Participant or Product Testing Programs.
    - 12 of the test cases (noted with an *) will fail for certain products that utilize incompatible / non-compliant technology stacks (e.g. Metro, CONNECT 3.3). These failures will be marked in the report with the Known Issue as Reason for Override

Participant Testing Notes:

- 2010 Participants will only run the Smoke Tests (SS:PRL-0000.0-2010)
- 2011 Participants will run the Smoke Test Service Set (SS: PRL-0000.0-2011) in addition to the MA Test Cases marked in the Participant Testing Column in the table on the following pages.

Product Testing Notes:

- 2011 Product Vendors will run the Smoke Test Service Set (SS: PRL-0000.0-2011) in addition to the MA Test Cases marked in the Product Testing Column in the table on the following pages.

Security Test Case List

Count	ID	Service Set	Scenario	Functional Area	Purpose/ Description	Participant Testing	Product Testing
1	3.000	SS: PRL-0006.0	TS: PRL-R-0006.0	SOAP security	Handle missing wsse:Security element	1	1
2	3.101	SS: PRL-0006.0	TS: PRL-R-0006.0	SOAP security	Handle missing Security/Timestamp element	1	1
3	3.201	SS: PRL-0006.0	TS: PRL-R-0035.0	WS-Addressing	Handle missing MessageID element		1

Count	ID	Service Set	Scenario	Functional Area	Purpose/ Description	Participant Testing	Product Testing
4	3.301 *	SS: PRL-0006.0	TS: PRL-R-0035.0	XML Signature	Handle missing Assertion signature element	1	1
5	3.302	SS: PRL-0006.0	TS: PRL-R-0036.0	XML Signature	Handle invalid Assertion signature	1	1
6	3.303	SS: PRL-0006.0	TS: PRL-R-0036.0	XML Signature	Handle missing timestamp signature element	1	1
7	3.306	SS: PRL-0006.0	TS: PRL-R-0037.0	XML Signature	Handle missing CanonicalizationMethod element in Timestamp signature	1	1
8	3.307	SS: PRL-0006.0	TS: PRL-R-0037.0	XML Signature	Handle missing CanonicalizationMethod algorithm in Timestamp signature	1	1
9	3.308	SS: PRL-0006.0	TS: PRL-R-0038.0	XML Signature	Handle missing SignatureMethod element in Timestamp signature	1	1
10	3.315	SS: PRL-0011.0	TS: PRL-R-0040.0	XML Signature	Handle missing DigestValue element in Timestamp signature reference	1	1
11	3.316	SS: PRL-0011.0	TS: PRL-R-0040.0	XML Signature	Handle Invalid DigestValue in Timestamp signature reference	1	1
12	3.317	SS: PRL-0011.0	TS: PRL-R-0041.0	XML Signature	Handle missing SignatureValue element in Timestamp signature	1	1
13	3.318	SS: PRL-0011.0	TS: PRL-R-0041.0	XML Signature	Handle missing KeyInfo element in timestamp signature		1
14	3.319	SS: PRL-0011.0	TS: PRL-R-0041.0	XML Signature	Handle missing KeyInfo/SecurityTokenReference element in timestamp signature		1
15	3.320 *	SS: PRL-0011.0	TS: PRL-R-0042.0	XML Signature	Handle missing /KeyInfo/SecurityToken Reference/@TokenType attribute in timestamp signature		1
16	3.321 *	SS: PRL-0011.0	TS: PRL-R-0042.0	XML Signature	Handle invalid TokenType version in timestamp signature		1
17	3.323	SS: PRL-0011.0	TS: PRL-R-0043.0	XML Signature	Handle missing /SecurityTokenReference/KeyIdentifier/@ValueType attribute in timestamp signature		1

Count	ID	Service Set	Scenario	Functional Area	Purpose/ Description	Participant Testing	Product Testing
18	3.324 *	SS: PRL-0011.0	TS: PRL-R-0043.0	XML Signature	Handle Invalid ValueType version in timestamp signature		1
19	3.325	SS: PRL-0011.0	TS: PRL-R-0043.0	XML Signature	Handle Invalid KeyIdentifier (AssertionID) in timestamp signature	1	1
20	3.326	SS: PRL-0011.0	TS: PRL-R-0044.0	XML Signature	Handle Missing KeyInfo in Assertion signature	1	1
21	3.401	SS: PRL-0012.0	TS: PRL-R-0046.0	SAML Assertion	Handle missing Assertion element	1	1
22	3.410 *	SS: PRL-0012.0	TS: PRL-R-0049.0	SAML Assertion	Handle Missing Issuer Format in Assertion		1
23	3.411 *	SS: PRL-0012.0	TS: PRL-R-0049.0	SAML Assertion	Handle Invalid Issuer Email Name ID in Assertion		1
24	3.412 *	SS: PRL-0012.0	TS: PRL-R-0049.0	SAML Assertion	Handle Invalid Issuer X.509 Name ID in Assertion		1
25	3.413 *	SS: PRL-0012.0	TS: PRL-R-0050.0	SAML Assertion	Handle Invalid Issuer Windows Name ID in Assertion		1
26	3.420	SS: PRL-0013.0	TS: PRL-R-0052.0	SAML Assertion	Handle Missing Subject element in Assertion		1
27	3.421 *	SS: PRL-0013.0	TS: PRL-R-0052.0	SAML Assertion	Handle Missing Subject Name ID in Assertion	1	1
28	3.422 *	SS: PRL-0013.0	TS: PRL-R-0053.0	SAML Assertion	Handle Invalid Subject Name ID in Assertion		1
29	3.423	SS: PRL-0013.0	TS: PRL-R-0053.0	SAML Assertion	Handle Missing Subject Confirmation in Assertion	1	1

Count	ID	Service Set	Scenario	Functional Area	Purpose/ Description	Participant Testing	Product Testing
30	3.424 *	SS: PRL-0013.0	TS: PRL-R-0053.0	SAML Assertion	Handle Missing Subject Confirmation Method in Assertion	1	1
31	3.426	SS: PRL-0013.0	TS: PRL-R-0054.0	SAML Assertion	Handle Missing Subject Confirmation Data in Assertion	1	1
32	3.427	SS: PRL-0013.0	TS: PRL-R-0054.0	SAML Assertion	Handle Missing Subject Confirmation Key Info in Assertion	1	1
33	3.429	SS: PRL-0013.0	TS: PRL-R-0055.0	SAML Assertion	Handle Invalid RSA Public Key Modulus in Assertion		1
34	3.430	SS: PRL-0013.0	TS: PRL-R-0055.0	SAML Assertion	Handle Missing RSA Public Key Exponent in Assertion		1
35	3.431	SS: PRL-0013.0	TS: PRL-R-0055.0	SAML Assertion	Handle Invalid RSA Public Key Exponent in Assertion		1
						19	**35**

For more details on the Participant or Product Testing Programs or the associated tools and checklists used, please visit: http://sequoiaproject.org/ehealth-exchange/testing-overview/testing-references-2/

These materials reflect the following:

- Change Log - The Official eHealth Exchange Specifications page lists, near the top, the Official Technical Errata and Change Log. This is the single authoritative source for changes to the Testing program, or specifications.

- Product Test Case Documentation - List of documents for the required and provisional eHealth Exchange Product Testing Program. Includes the applications required and listing of all product test cases, documentation, provisional tests, conformity assessment checklists, Testing data load set and documents, and a description of content tests.

- Participant Testing Program Overview - A broad overview of the process, applications and documentation for the Participant Testing Program. List of all participant test cases, documentation, provisional tests, conformity assessment checklists, Testing data load sets and documents and a description of content tests for the current eHealth Exchange Participant Testing Program

- Sequoia Project/AEGIS Developers Integration Lab (DIL) Guides

Version 2 Change Updates

Changes that have been made since the initial publication of this document (July 2013):

1. Combined Required Security Testing Documentation for both Participant and Product Testing Programs for the eHealth Exchange 2011 Programs.
2. Updated Service Set, Test Scenario and Test Case Revision to Version 2 with date format
3. Updated Data Load reference to DS: PRL-2
4. Changed reference for 2010 Exchange from true to false *(Security tests only apply to 2011 specifications)*
5. Updated logo and copyright information at header and footer of document
6. Applied proper formatting to all tables
7. Updated change history.

eHealth Exchange™

eHealth Exchange Required Security Testing

Service Set

Development Requirement Specification

Service Set ID:	SS: PRL-0006.0
Version:	17
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This Service Set contains 2011 Scenarios with MP/AF (MA) Error Test Cases for the System Under Test (SUT) as the Responder Actor.

Test Data

Data Load Set

DS: PRL-2

Test Scenarios

TS: PRL-R-0006.0
TS: PRL-R-0035.0
TS: PRL-R-0036.0
TS: PRL-R-0037.0
TS: PRL-R-0038.0

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0006.0
Version:	27
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set

DS: PRL-2

Data Notes

See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.000 using patient P-000000002
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.101 using patient P-000000005

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.000
Title:	Handle missing wsse:Security element
Release Date:	Revised 141210 - Version 2
Version:	13
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing wsse:Security element.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000002

Test Case Metadata Association
D-000000002.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element wsse:Security is missing.
   $XDSDocumentEntryPatientID = [patient P-000000002]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Messaging Platform 3.0 Sec 3.6.2
2011 Underlying Specification	SOAP 1.2: Table 4 WS-Addressing 1.0, SOAP Binding: Section 6 WSS SOAP Message Security 1.1: Lines 2038-2044

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.101
Title:	Handle missing Security/Timestamp element
Release Date:	Revised 141210 - Version 2
Version:	20
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Security/Timestamp element.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000005

Test Case Metadata Association
D-000000005.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except

   the SOAP header element Security/Timestamp is missing.

$XDSDocumentEntryPatientID = [patient P-000000005]
$XDSDocumentEntryStatus = Approved
returnType = LeafClass
SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.2
2011 Underlying Specification	Web Services Security: SAML Token Profile 1.1 specification

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0035.0
Version:	14
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set

DS: PRL-2

Data Notes

See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.201 using patient P-000000015
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.301 using patient P-000000019

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.201
Title:	Handle missing MessageID element
Release Date:	Revised 141210 - Version 2
Version:	17
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing MessageID element.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None
Test Case Patient Association
P-000000015

Test Case Metadata Association
D-000000015.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element MessageID is missing.

$XDSDocumentEntryPatientID = [patient P-000000015]
$XDSDocumentEntryStatus = Approved
returnType = LeafClass
SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

   NOTE: The DIL is unable to connect the Response to the Test Case because the MessageID is missing. Due to this, the Test Case will remain in an initiated state. The user should go to the "Gateway Transactions" screen in the DIL, click the "Open" link for the Response message that corresponds to this Test Case and save it as an XML format with the following naming convention "TC: MAQD-R-0003.201-2011_[Participant Name]_Response.xml". Once the Response has been saved, the user should go back to the Test Case Result for this test case and click on the "Attach Document" button. The user should select the XML Response message they just downloaded and saved and upload it to the Test Case. The Validator will be looking for the attachment to the Test Case before being able to manually pass the Test Case.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Messaging Platform 3.0 Section 3.5
2011 Underlying Specification	Web Services Addressing 1.0

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.301
Title:	Handle missing assertion signature element
Release Date:	Revised 141210 - Version 2
Version:	11
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Security/Assertion/Signature element.

Preconditions

Data Load Set

DS: PRL-2

Data Notes

None

Test Case Patient Association

P-000000019

Test Case Metadata Association

D-000000019.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters,
   **except the SOAP header element Security/Assertion/Signature is missing.
   $XDSDocumentEntryPatientID = [patient P-000000019]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - ◦ MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - ◦ CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3.4
2011 Underlying Specification	W3CExclusive XML Canonicalization Version 1.0 specification

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0036.0
Version:	11
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set

DS: PRL-2

Data Notes

See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.302 using patient P-000000023
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.303 using patient P-000000026

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.302
Title:	Handle invalid assertion signature
Release Date:	Revised 141210 - Version 2
Version:	12
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with an incorrect Security/Assertion/Signature.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000023

Test Case Metadata Association
D-000000023.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters,
   **except the SOAP header element Security/Assertion/Signature is incorrect. Specifically, the SignatureValue does not allow the signature to be verified.
   $XDSDocumentEntryPatientID = [patient P-000000023]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3.4
2011 Underlying Specification	W3CExclusive XML Canonicalization Version 1.0 specification

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.303
Title:	Handle missing timestamp signature element
Release Date:	Revised 141210 - Version 2
Version:	11
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Security/Signature (for Timestamp) element.

Preconditions

Data Load Set

DS: PRL-2

Data Notes

None

Test Case Patient Association

P-000000026

Test Case Metadata Association

D-000000026.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters,
   **except the SOAP header element Security/Signature (for Timestamp) is missing.
   $XDSDocumentEntryPatientID = [patient P-000000026]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.2
2011 Underlying Specification	OASIS XSPA profile of SAML

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0037.0
Version:	8
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set

DS: PRL-2

Data Notes

See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.306 using patient P-000000039
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.307 using patient P-000000042

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.306
Title:	Handle missing CanonicalizationMethod element in Timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	10
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Security/Signature/SignedInfo/CanonicalizationMethod element.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000039

Test Case Metadata Association
D-000000039.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters,
   **except the SOAP header element Security/Signature/SignedInfo/CanonicalizationMethod is missing.
   $XDSDocumentEntryPatientID = [patient P-000000039]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.2
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.307
Title:	Handle missing CanonicalizationMethod algorithm in Timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	10
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Security/Signature/SignedInfo/CanonicalizationMethod/@algorithm element.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000042

Test Case Metadata Association
D-000000042.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters,
   **except the SOAP header element
   Security/Signature/SignedInfo/CanonicalizationMethod/@algorithm is missing.
   $XDSDocumentEntryPatientID = [patient P-000000042]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.4
2011 Underlying Specification	W3CExclusive XML Canonicalization Version 1.0 specification

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0038.0
Version:	14
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.308 using patient P-000000045

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.308
Title:	Handle missing SignatureMethod element in Timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	10
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing SignatureMethod element in Timestamp signature.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000045

Test Case Metadata Association
D-000000045.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **exceptthe SOAP header element
   Security/Signature/SignedInfo/SignatureMethod is missing.
   $XDSDocumentEntryPatientID = [patient P-000000045]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.4
2011 Underlying Specification	W3CExclusive XML Canonicalization Version 1.0 specification

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Service Set

Development Requirement Specification

Service Set ID:	SS: PRL-0011.0
Version:	17
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This Service Set contains 2010/2011 Scenarios with MP/AF (MA) Error Test Cases for the System Under Test (SUT) as the Responder Actor.

Test Data

Data Load Set
DS: PRL-2

Test Scenarios

TS: PRL-R-0040.0
TS: PRL-R-0041.0
TS: PRL-R-0042.0
TS: PRL-R-0043.0
TS: PRL-R-0044.0

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0040.0
Version:	13
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.315 using patient P-000000005
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.316 using patient P-000000008

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.315
Title:	Handle missing DigestValue element in Timestamp signature reference
Release Date:	Revised 141210 - Version 2
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Security/Signature/SignedInfo/Reference/DigestValue element.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000005

Test Case Metadata Association
D-000000005.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element
   Security/Signature/SignedInfo/Reference/DigestValue is missing.
   $XDSDocumentEntryPatientID = [patient P-000000005]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   ◦ MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   ◦ CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.2
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.316
Title:	Handle Invalid DigestValue in Timestamp signature reference
Release Date:	Revised 141210 - Version 2
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with
a Security/Signature/SignedInfo/Reference/DigestValue element with an invalid value.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000008

Test Case Metadata Association
D-000000008.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element
   Security/Signature/SignedInfo/Reference/DigestValue element has an invalid value
   $XDSDocumentEntryPatientID = [patient P-000000008]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.2
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0041.0
Version:	13
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.317 using patient P-000000011
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.318 using patient P-000000015
3. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.319 using patient P-000000019

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.317
Title:	Handle missing SignatureValue element in Timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Security/Signature/SignatureValue element.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000011

Test Case Metadata Association
D-000000011.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element
   Security/Signature/SignatureValue is missing.
   $XDSDocumentEntryPatientID = [patient P-000000011]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.4
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.318
Title:	Handle missing KeyInfo element in timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	10
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Security/Signature/KeyInfo element.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000015

Test Case Metadata Association

D-000000015.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters,
   **except the SOAP header element
   Security/Signature/KeyInfo is missing.
   $XDSDocumentEntryPatientID = [patient P-000000015]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:

   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3.4.3
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.319
Title:	Handle missing KeyInfo/SecurityTokenReference element in timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Security/Signature/KeyInfo/SecurityTokenReference element.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000019

Test Case Metadata Association
D-000000019.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

    SOAP Header = MP: MA Default Request (TestTool) Message Parameters,
    **except the SOAP header element Security/Signature/KeyInfo/SecurityTokenReference
    is missing.
    $XDSDocumentEntryPatientID = [patient P-000000019]
    $XDSDocumentEntryStatus = Approved returnType
    = LeafClass
    SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

    OR

    Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
    - MP: MA Fault (Both) Message Parameters

    OR

    Verify conformance of the PD Response to the:

    - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3.4.3
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0042.0
Version:	11
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.320 using patient P-000000023
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.321 using patient P-000000026

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.320
Title:	Handle missing /KeyInfo/SecurityTokenReference/@TokenType attribute in timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	10
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Security/Signature/KeyInfo/SecurityTokenReference/@TokenTypeelement.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000023

Test Case Metadata Association
D-000000023.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters,
   **except the SOAP header attribute
   Security/Signature/KeyInfo/SecurityTokenReference/@TokenType is missing.
   $XDSDocumentEntryPatientID = [patient P-000000023]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:

   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.2
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.321
Title:	Handle invalid TokenType version in timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with an invalid TokenType version in timestamp signature.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000026

Test Case Metadata Association
D-000000026.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters,
   **except the SOAP header attribute Security/Signature/KeyInfo/@TokenType is invalid - "http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1".
   $XDSDocumentEntryPatientID = [patient P-000000026]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:

   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.2
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0043.0
Version:	12
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.323 using patient P-000000031
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.324 using patient P-000000039
3. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.325 using patient P-000000042

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.323
Title:	Handle missing /SecurityTokenReference/KeyIdentifier/@ValueType attribute in timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	8
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing /SecurityTokenReference/KeyIdentifier/@ValueType attribute in timestamp signature.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000031

Test Case Metadata Association

D-000000031.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header attribute Security/Signature/KeyInfo/SecurityTokenReference/KeyIdentifier/@ValueType is missing.
   $XDSDocumentEntryPatientID = [patient P-000000031]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:

   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.2
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.324
Title:	Handle Invalid ValueType version in timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	8
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with an invalid ValueType version in timestamp signature.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000039

Test Case Metadata Association

D-000000039.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header attribute
   Security/Signature/KeyInfo/SecurityTokenReference/KeyIdentifier/@ValueType is invalid - "http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID".
   $XDSDocumentEntryPatientID = [patient P-000000039]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:

   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.2
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.325
Title:	Handle Invalid KeyIdentifier (assertionID) in timestamp signature
Release Date:	Revised 141210 - Version 2
Version:	8
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with an invalid KeyIdentifier (assertionID) in timestamp signature.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000042

Test Case Metadata Association
D-000000042.1

Test Steps

The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Signature/KeyInfo/SecurityTokenReference/KeyIdentifier is invalid: "XXXXXX", which does not resolve to anything.
$XDSDocumentEntryPatientID = [patient P-000000042]
$XDSDocumentEntryStatus = Approved returnType = LeafClass
SOAP request = synchronous

Expected Result: The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

OR

Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

Verify conformance of the fault Response message to the:

- MP: MA Fault (Both) Message Parameters

OR

Verify conformance of the PD Response to the:

- CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.2.2
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0044.0
Version:	11
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.326 using patient P-000000045

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.326
Title:	Handle Missing KeyInfo in assertion signature
Release Date:	Revised 141210 - Version 2
Version:	7
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing KeyInfo in assertion signature.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000045

Test Case Metadata Association
D-000000045.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Signature/KeyInfo is missing.
   $XDSDocumentEntryPatientID = [patient P-000000045]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   ◦ MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the PD Response to the:
   ◦ CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3.4.3
2011 Underlying Specification	

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Service Set

Development Requirement Specification

Service Set ID:	SS: PRL-0012.0
Version:	18
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This Service Set contains 2010/2011 Scenarios with MP/AF (MA) Error Test Cases for the System Under Test (SUT) as the Responder Actor.

Test Data

Data Load Set
DS: PRL-2

Test Scenarios

TS: PRL-R-0046.0

TS: PRL-R-0049.0

TS: PRL-R-0050.0

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0046.0
Version:	12
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.401 using patient P-000000002

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.401
Title:	Handle missing Assertion element
Release Date:	Revised 141210 - Version 2
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Assertion element.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000002

Test Case Metadata Association
D-000000002.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion is missing.
   $XDSDocumentEntryPatientID = [patient P-000000002]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SOAP Message Security 1.1: Section 12

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0049.0
Version:	12
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.410 using patient P-000000031
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.411 using patient P-000000039
3. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.412 using patient P-000000042

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.410
Title:	Handle Missing Issuer Format in Assertion
Release Date:	Revised 141210 - Version 2
Version:	10
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Issuer Format in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000031

Test Case Metadata Association
D-000000031.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Issuer/@Format is missing.
   $XDSDocumentEntryPatientID = [patient P-0000000031]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:

   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SAML Token Profile 1.1: Section 3.6

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.411
Title:	Handle Invalid Issuer Email Name ID in Assertion
Release Date:	Revised 141210 - Version 2
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Issuer Email Name ID in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000039

Test Case Metadata Association
D-000000039.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except 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.
   $XDSDocumentEntryPatientID = [patient P-0000000039]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:

   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SAML Token Profile 1.1: Section 3.6; SAML Core 2.0: Section 8.3.2

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.412
Title:	Handle Invalid Issuer X.509 Name ID in Assertion
Release Date:	New 130130 - Version Vendor
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Issuer X.509 Name ID in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000042

Test Case Metadata Association
D-000000042.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except 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.
   $XDSDocumentEntryPatientID = [patient P-0000000042]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   ◦ MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:

   ◦ CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SAML Token Profile 1.1: Section 3.6; SAML Core 2.0: Section 8.3.3

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0050.0
Version:	12
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.413 using patient P-000000045

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.413
Title:	Handle Invalid Issuer Windows Name ID in Assertion
Release Date:	New 130130 - Version Vendor
Version:	8
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Issuer Windows Name ID in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000045

Test Case Metadata Association
D-000000045.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except 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.
   $XDSDocumentEntryPatientID = [patient P-0000000045]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:

   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SAML Token Profile 1.1: Section 3.6; SAML Core 2.0: Section 8.3.4

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Service Set

Development Requirement Specification

Service Set ID:	SS: PRL-0013.0
Version:	14
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This Service Set contains 2010/2011 Scenarios with MP/AF (MA) Error Test Cases for the System Under Test (SUT) as the Responder Actor.

Test Data

Data Load Set
DS: PRL-2

Test Scenarios

TS: PRL-R-0052.0
TS: PRL-R-0053.0
TS: PRL-R-0054.0

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0052.0
Version:	12
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.420 using patient P-000000005
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.421 using patient P-000000008

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.420
Title:	Handle Missing Subject element in Assertion
Release Date:	Revised 141210 - Version 2
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Subject element in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000005

Test Case Metadata Association
D-000000005.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Subject is missing.
   $XDSDocumentEntryPatientID = [patient P-0000000005]
   $XDSDocumentEntryStatus = Approved returnType =
   LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   ◦ MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:

   ◦ CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SOAP Message Security 1.1: Section 12

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.421
Title:	Handle Missing Subject Name ID in Assertion
Release Date:	Revised 141210 - Version 2
Version:	8
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Subject Name ID element in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000008

Test Case Metadata Association
D-000000008.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Subject/NameID is missing.
   $XDSDocumentEntryPatientID = [patient P-0000000008]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SOAP Message Security 1.1: Section 12

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0053.0
Version:	13
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.422 using patient P-000000011
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.423 using patient P-000000015
3. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.424 using patient P-000000019

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.422
Title:	Handle Invalid Subject Name ID in Assertion
Release Date:	Revised 141210 - Version 2
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with an invalid Subject Name ID in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000011

Test Case Metadata Association
D-000000011.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Subject/NameID/@Format is something other than the two allowed formats, emailAddress and X509SubjectName.
   $XDSDocumentEntryPatientID = [patient P-0000000011]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:

   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SOAP Message Security 1.1: Section 12

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.423
Title:	Handle Missing Subject Confirmation in Assertion
Release Date:	Revised 141210 - Version 2
Version:	8
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Subject Confirmation element in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000015

Test Case Metadata Association
D-000000015.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Subject/SubjectConfirmation is missing.
   $XDSDocumentEntryPatientID = [patient P-0000000015]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SOAP Message Security 1.1: Section 12

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.424
Title:	Handle Missing Subject Confirmation Method in Assertion
Release Date:	Revised 141210 - Version 2
Version:	8
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Subject Confirmation Method element in Assertion**.**

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000019

Test Case Metadata Association
D-000000019.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Subject/SubjectConfirmation/@Method is missing.
   $XDSDocumentEntryPatientID = [patient P-0000000019]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   ◦ MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:
   ◦ CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SOAP Message Security 1.1: Section 12

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0054.0
Version:	12
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.426 using patient P-000000023
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.427 using patient P-000000026

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.426
Title:	Handle Missing Subject Confirmation Data in Assertion
Release Date:	Revised 141210 - Version 2
Version:	8
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Subject Confirmation Data element in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000023

Test Case Metadata Association
D-000000023.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Subject/SubjectConfirmation/SubjectConfirmationDat is missing.
   $XDSDocumentEntryPatientID = [patient P-0000000023]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SOAP Message Security 1.1: Section 12

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.427
Title:	Handle Missing Subject Confirmation Key Info in Assertion
Release Date:	Revised 141210 - Version 2
Version:	8
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing Subject Confirmation Key Info element in Assertion**.**

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000026

Test Case Metadata Association
D-000000026.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Subject/SubjectConfirmation/SubjectConfirmationData/KeyInfo is missing.
   $XDSDocumentEntryPatientID = [patient P-0000000026]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:
   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:
   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SOAP Message Security 1.1: Section 12

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Scenario

Development Requirement Specification

Test Scenario ID:	TS: PRL-R-0055.0
Version:	12
Release:	Revised 141210 - Version 2

Coverage Specifications

2011 Exchange:	True
2010 Exchange:	False

Purpose/Description

This scenario is a collection of MA Responder error flow test case PD/QD/RD sequences that confirm the SUT correctly responds to a variety of error requests from an Initiator (the Testing Tool).

Preconditions

Data Load Set
DS: PRL-2

Data Notes
See data instructions for each Test Case.

Scenario Steps

1. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.429 using patient P-000000031
2. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.430 using patient P-000000039
3. Execute TC: PD-R-0000.0 variant + TC: MAQD-R-0003.431 using patient P-000000042

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.429
Title:	Handle Invalid RSA Public Key Modulus in Assertion
Release Date:	Revised 141210 - Version 2
Version:	10
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with an invalid RSA Public Key Modulus in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000031

Test Case Metadata Association
D-000000031.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Subject/SubjectConfirmation/SubjectConfirmationData/KeyInfo/KeyValue/RSA KeyValue/Modulus does not contain the modulus from the RSA public key embedded in the certificate assigned to the sending system.
   $XDSDocumentEntryPatientID = [patient P-0000000031]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   ◦ MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:

   ◦ CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SAML Token Profile 1.1: Section 3.6

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.430
Title:	Handle Missing RSA Public Key Exponent in Assertion
Release Date:	Revised 141210 - Version 2
Version:	10
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with a missing RSA Public Key Exponent element in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000039

Test Case Metadata Association
D-000000039.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element Security/Assertion/Subject/SubjectConfirmation/SubjectConfirmationData/KeyInfo/KeyValue/RSA KeyValue is present, but does not contain an <Exponent> element.
   $XDSDocumentEntryPatientID = [patient P-0000000039]
   $XDSDocumentEntryStatus = Approved returnType
   = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   ◦ MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:

   ◦ CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SOAP Message Security 1.1: Section 12

Change History	
Date	**Author**
December 10, 2014	Didi Davis

eHealth Exchange™

eHealth Exchange Required Security Testing

Test Case

Development Requirement Specification

Test Case ID:	TC: MAQD-R-0003.431
Title:	Handle Invalid RSA Public Key Exponent in Assertion
Release Date:	Revised 141210 - Version 2
Version:	9
SUT Role:	Responder

Coverage Specifications

2011 Exchange:	true
2010 Exchange:	false
IHE Profile:	
Flow:	Error
Optionality:	Required

Purpose/Description

Testing Tool sends a simple QD Request to the System with an invalid RSA Public Key Exponent in Assertion.

Preconditions

Data Load Set
DS: PRL-2

Data Notes
None

Test Case Patient Association
P-000000042

Test Case Metadata Association
D-000000042.1

Test Steps

1. The Testing Tool sends a synchronous Find Documents Request to the System, using the following required parameters:

   SOAP Header = MP: MA Default Request (TestTool) Message Parameters, **except the SOAP header element
   Security/Assertion/Subject/SubjectConfirmation/SubjectConfirmationData/KeyInfo/KeyValue/RSAKeyValue/Exponent does not contain the exponent from the RSA public key embedded in the certificate assigned to the sending system.
   $XDSDocumentEntryPatientID = [patient P-0000000042]
   $XDSDocumentEntryStatus = Approved
   returnType = LeafClass
   SOAP request = synchronous

2. **Expected Result:** The System returns a SOAP fault to the Testing Tool with text describing the internal error using MP: MA Fault (Both) Message Parameters.

   OR

   Based on its security policy, instead of returning a fault the System may return a normal response, but without performing the requested action. Example: if the request were a Patient Discovery, a normal response is returned, but with no matching patients found. This approach of concealing the fault is permitted by the underlying requirements to mitigate certain kinds of attacks.

3. Verify conformance of the fault Response message to the:

   - MP: MA Fault (Both) Message Parameters

   OR

   Verify conformance of the QD Response to the:

   - CL: MA SOAP Response Checklist

Referenced Specifications

2011 Exchange Specification	Authorization Framework 3.0 Sec 3.3
2011 Underlying Specification	SAML Token Profile 1.1: Section 3.6

Change History	
Date	**Author**
December 10, 2014	Didi Davis