Nationwide Health Information Network (NHIN)

Authorization Framework
Specification

V 3.0

7/27/2011

Contributors

Name	NHIO Represented	Organization
Richard Franck	NCHICA	IBM
Tony Mallia	Fed NHIO	VA
Victoria Vickers	Fed NHIO	FHA
Deborah Lafky	ONC/NHIN	ONC
David Riley	FHA	FHA
Tom Davidson	SSA	SSA
Richard Kernan	ONC/NHIN	Deloitte
Jackie Key	ONC/NHIN	Deloitte
Eric Heflin	NHIN, Chair Security and Privacy Workgroup	Medicity/IHE/HITSP
Seonho Kim		ApeniMED, Inc
Scott Robertson	Kaiser Permanente	Kaiser Permanente
Sandy Stuart	Kaiser Permanente	Kaiser Permanente
Michael Nenashev	ONC/NHIN	Lockheed Martin
Les Westberg	ONC/NHIN	AgileX
John Moehrke		GE Healthcare/IHE/HL7
Joan DuHaime	ONC/NHIN	Lockheed Martin
Joe Lamy	ONC/NHIN	The Nitor Group
Jeff Tunkel	ONC/NHIN	Lockheed Martin
George Varghese	ONC/NHIN	Deloitte
Didi Davis	ONC/NHIN	Deloitte, Serendipity Health
David Roberts	Wright State University	Wright State University
Dave Arvin	SSA	SSA
David Morris	ONC/NHIN	Lockheed Martin
Dan Vigano	ONC/NHIN	Deloitte
Chuck Hagan	ONC/NHIN	Deloitte
Benson Chang	ONC/NHIN	Deloitte
Amram Ewoo	ONC/NHIN	Deloitte
Josh Abraham	SSA	SSA
John Donnelly		IntePro Solutions
Shrikant Gajengi	SSA	SSA
Saadi Mirza	SSA	SSA

Document Change History

Version	Date	Changed By	Items Changed Since Previous Version
1.4	4/16/08	Tony Mallia, Richard Franck	
1.4.1	4/29/08	Deborah Lafky	Format, preparation for HITSP review
1.5	5/22/08	Tony Mallia, Richard Franck	Change User Role codes to SNOMED CT
1.6	7/22/2008	David L. Riley	Added Appendix A: SAML Rules and Appendix B: Sample Messages
1.7	10/07/08	Dave Riley Victoria Vickers	Integrated in decisions regarding ws-Security elements, <Issuer> and <Subject> elements, Role and PurposeForUse <AttributeValue> elements
1.8	11/18/2008	Richard Franck	Changes related to SSA Authorized Release of Information use case; editing and clean up

Version	Date	Changed By	Items Changed Since Previous Version
1.9	11/24/2008	Victoria Vickers	Addition of descriptions to support Digital Signatures
1.9.1	01/30/2009	David L. Riley	Minor edits to prepare for publication
1.9.2 [1]	8/11/2009	Richard Franck	Modified to be consistent with XSPA profile of SAML
1.9.21	9/3/2009	Richard Franck	Added attribute for Home Community ID
1.9.22	9/24/2009	Tom Davidson	Added XSPA attribute resource-id Change Subject Discovery to Patient Discovery Removed references to Audit Log Query Specification. Changes to Authorization Decision Statement attribute to support HITSP TP30. Removed references to SSA Use Case. SSA Use Case Implementation guide should refer to this specification.
1.9.23	11/3/2009	Tom Davidson, Richard Franck	Fixed errors; noted deprecated attributes from Trial Implementation.
2.0	1/29/2010	Tom Davidson, Richard Franck, Rich Kernan Jackie Key	Added NPI attribute. Changed namespace for Authorization Decision Statement action. Applied consistent formatting/language and enhanced clarity.
2.0.1	9/17/2010	Eric Heflin	Added SAML PurposeForUse vs. PurposeOfUse AttributeValue implementation note. Caution: Pending potentially breaking change. Please read this section carefully.
2.0.2	5/24/2011	George Varghese, Tom Davidson, John Moehrke, Joe Lamy, Didi Davis, Benson Chang, Eric Heflin	Substantive changes in yellow highlighting. Partially updated NHIN to long form name. Updated PurposeOfUse examples and associated non-normative implementation guidance. Corrected/updated references. Removed transport binding implied requirement. Corrected SAML 2.0 non-normative diagram element order and removed associated table. Various editorial improvements (added figure/table numbers, formatting, etc.) Removed Appendix A. Added SAML 2.0 Assertion ID data type clarification. Added SAML 2.0 <Issuer> intended use clarification. Added requirement to use W3C Exclusive Canonicalization for XML-DSig.
2.0.3	6/20/2011	Chuck Hagan	Correction of example in section 3.3.2.9
2.0.4	7/5/2011	Eric Heflin	Updated text in section 3.2.2 Timestamp.
2.0.5	7/11/2011	Eric Heflin, Chuck Hagan	Additional clarifications added to Sections 1.1, 3.2 and 3.3, editorial improvements. Fixed URL error for W3C ID data type reference document in section 3.3 item 2.

[1] These unpublished draft versions have been re-numbered to conform to subsequently defined versioning conventions.

Version	Date	Changed By	Items Changed Since Previous Version
2.0.6	7/15/2011	Spec Factory Security and Privacy Workgroup	Added new content in section 3.3 documenting that the NHIN requires a HOK subject confirmation method at this time. Added a clarification related to the certificate used to sign <Timestamp> and <saml> apexes. Editorial issues. Changed a typographical error in section 1.5 where “asynchronous” was used instead of the correct “deferred” message exchange pattern. Added caution to implementers regarding the xacml:2.0 identifier text in section 3.3.2.7. Clarified the use of attributes in section 3.3.2.
2.0.7	7/22/2011	Spec Factory Security and Privacy Workgroup	Updated contributors list. Edited word spacing used in text of PurposeOfUse. Clarified OASIS specification reference in Section 3.2.2.
3.0	7/27/2011	ONC	Finalized for Production Publication

Document Approval

Version	Date	Approved By	Role
1.6	10/6/2008	NHIN Cooperative Technical and Security Working Group	Approves all specifications for production NHIN use
2.0	1/25/2010	NHIN Technical Committee	Approves all specifications for production NHIN use
2.0.1	2/1/2011	NHIN Technical Committee	Approves all specifications for production NHIN use
2.0.7	7/25/2011	NHIN Technical Committee	Approves all specifications for production NHIN use

Substantial content changes to the specification relevant to this new publication version have been highlighted in yellow within the documentation to help implementers identify requirements that may affect industry implementations.

Table of Contents

1 Preface

1.1 Introduction

The Nationwide Health Information Network (NHIN) Foundation specifications define the primary set of services and protocols needed to establish a messaging, security, and privacy foundation for the NHIN. It is upon this foundation that the functional set of Nationwide Health Information Network web service interfaces operates.

This specification does not describe a web service interface. Instead, it defines the required exchange of information describing the initiator of a request between Health Information Organizations (HIOs) participating as nodes on the Nationwide Health Information Network. The purpose of this information exchange is to enable a responding NHIO to evaluate the request based on the information contained in the initiating NHIOs assertions and its own local policies and permissions. This Authorization Framework specification is foundational to the Nationwide Health Information Network and applies to every message.

This specification does not intend to conflict with any referenced underlying normative standards. The intent is only to constrain for the purposes of Nationwide Health Information Network interoperability.

1.2 Intended Audience

The primary audiences for Nationwide Health Information Network Specifications are the individuals responsible for implementing software solutions that realize these interfaces at Health Information Organizations (HIOs) who are, or seek to be, nodes on the Nationwide Health Information Network. HIOs, which act as nodes on the Nationwide Health Information Network, are termed NHIOs. This specification document is intended to provide an understanding of the context in which the web service interface is meant to be used, the behavior of the interface, the Web Services Description Language (WSDLs) used to define the service, and any Extensible Markup Language (XML) schemas used to define the content.

The examples, figures and tables in this specification are non-normative unless labeled otherwise. Implementers are advised to not treat these non-normative sections as normative. In the event that non-normative examples, figures and tables disagree with normative text, the normative text is authoritative.

1.3 Business Needs Supported by this Specification

In order to evaluate a request sent by an initiating Nationwide Health Information Network node, a responding NHIO must be supplied with a standard set of information, which characterizes the initiator of the request. The Nationwide Health Information Network Authorization Framework specification defines this information as well as the mechanism for its exchange.

Further, the Authorization Framework is required to support two of the Nationwide Health Information Network's central design principles:

Local Autonomy – acknowledges that the decision to release information from one Nationwide Health Information Network node to another is a local decision is governed by Federal and State regulations and local policies and permissions specific to the responding node. Given this principle, Nationwide Health Information Network transactions must include information about the requestor (or sender, depending on whether it is a push or pull transaction) in order to enable the responding node to make a decision about whether to participate in the requested information exchange.

Local Accountability - each Nationwide Health Information Network node is accountable for the accuracy of the information it provides to assist the decision making process embodied in the local autonomy principle. This includes end-user authentication assertions.

Together with the Nationwide Health Information Network Messaging Platform, this specification is part of the NHIN's messaging, security, and privacy foundation. All other service interface specifications assume this foundation.

1.4 Referenced Documents and Standards

The following documents and standards were referenced during the development of this specification. Deviations from or constraints upon these standards are identified below.

1) **Org/SDO name:** OASIS

   Reference # / Spec Name: Assertions and Protocols for Security Assertion Markup Language (SAML)

   Version #: v2.0

   Underlying Specs:

   Nationwide Health Information Network Deviations or Constraints:

   Link: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

2) **Org/SDO name:** OASIS

   Reference # / Spec Name: Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare

   Version #: v1.0

   Underlying Specs:

   Nationwide Health Information Network Deviations or Constraints:

   Link: http://www.oasis-open.org/committees/download.php/33396/saml-xspa-1%200-cd04.doc

3) **Org/SDO name:** OASIS

   Reference # / Spec Name: Authentication Context for Security Assertion Markup Language (SAML)

   Version #: v2.0

   Underlying Specs:

   Nationwide Health Information Network Deviations or Constraints:

   Link: http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

4) **Org/SDO name:** OASIS

   Reference # / Spec Name: Web Services Security: SOAP Message Security

Version #: v1.1 (WS-Security 2004)

Underlying Specs:

Nationwide Health Information Network Deviations or Constraints:

Link: http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

5) **Org/SDO name:** WS-I

Reference # / Spec Name: Security Profile

Version #: v1.1

Underlying Specs:

- Transport Layer Security v1.0
- XML Signature v1.0
- Web Services Description Language (WSDL) v1.1
- Symmetric Encryption Algorithm and Key Length AES 128-bit
- X.509 Token Profile v1.0
- Attachment Security v1.0

Link: http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html

6) **Org/SDO name:** OASIS

Reference # / Spec Name: Web Services Security: SAML Token Profile

Version #: v1.1

Underlying Specs:

Nationwide Health Information Network Deviations or Constraints:

Link: http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf

1.5 Relationship to Other Nationwide Health Information Network Specifications

This specification is related to other Nationwide Health Information Network specifications as described below.

- **Messaging Platform –** specifies a base set of messaging standards and web service protocols, which must be implemented by each Nationwide Health Information Network node and applies to all transactions. Together with the Messaging Platform, the Authorization Framework defines the foundational messaging, security and privacy mechanisms for the Nationwide Health Information Network.

The Authorization Framework is not specifically related as part of a transaction to the Nationwide Health Information Network Discovery and Information Exchange Services. Rather, it describes the information, which must accompany the requests enabled by each of these Nationwide Health Information Network web services. SAML 2.0 assertions are only required for requests from an initiating gateway to a responding gateway; SAML 2.0 assertions are not required for synchronous responses from a responding gateway to an initiating gateway. SAML 2.0 assertions are required for deferred responses (which are essentially a new request).

2 Framework Description

2.1 Definition

The Authorization Framework defines the exchange of metadata used to characterize the initiator of a Nationwide Health Information Network request so that it may be evaluated by responding NHIOs in local authorization decisions.

Along with the Messaging Platform, this specification forms the Nationwide Health Information Network's messaging, security, and privacy foundation. It employs SAML 2.0 assertions

The purpose of this exchange is to provide the responder with the information needed to make an authorization decision for the requested function. Each initiating message must convey information regarding end user attributes and authentication using SAML 2.0 assertions.

Note that the term "Subject" in SAML and XACML refers to the individual making the request. In this specification, the term "User" is generally used with the same meaning, but when referring to attributes defined in SAML or XACML, the naming convention of the standard is retained.

2.1.1 Request Definition

Nationwide Health Information Network requests are defined by the applicable service interface, the interface operation, and the identity of the record target (unambiguous person identity in the responding NHIO, when known).

2.1.2 Identity of the Record Target

In most Nationwide Health Information Network requests, Patient Discovery a notable exception, the record target is the unambiguous person identity in the responding NHIO. The assertion contained in the Authorization Framework declares that the initiating user is authorized by the initiating NHIO to access information about this person. It is also required for HIPAA Privacy Disclosure Accounting.

2.2 Design Principles and Assumptions

The following assumptions or design principles underlie this specification:

- All inter-node requests on the Nationwide Health Information Network must utilize the Authorization Framework.
- There is not assumed to be Cross Provisioning of users between NHIOs. That is, human end users are not expected or required to have identities defined in any NHIO security domain other than in the NHIO initiating a request. This principle is designed to avoid the need for the difficult process of synchronizing end-user identities across organizational boundaries.
- The initiating NHIO is required to and is responsible for the authentication and authorization of its users. Refer to Local Accountability, as described in section 1.3 of this specification.
- The responding NHIO uses the information conveyed via the Authorization Framework to inform its local authorization decision. Refer to Local Autonomy, as described in section 1.3 of this specification.
- NHIO architectures are decoupled and externally opaque. While each NHIO must conform to the Nationwide Health Information Network messaging, security, and privacy foundations for inter-NHIO transactions, internal security mechanisms and standards are to be defined by each NHIO.
- The initiating NHIO must include all REQUIRED attributes in each request. It is at the discretion of the receiving NHIO to decide which attributes to consider in its local authorization decision

- The assertion attribute definitions specified in this document are not intended to be an exhaustive and restrictive list of attributes that may be specified in the SAML assertions. Additionally, this document recognizes that some integration profiles may have a need for custom assertion statements, and does not preclude their use.

2.3 Triggers

Nationwide Health Information Network Authorization Framework is central to the messaging, security, and privacy foundation. All Nationwide Health Information Network requests must conform to this specification.

2.4 Transaction Standard

The Nationwide Health Information Network Authorization Framework is based on the Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, the Authentication Context for SAML V2.0, the Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML for Healthcare Version 1.0 and the OASIS Web Services Security: SAML Token Profile 1.1 specifications. (Note: Web Services Security SAML Token Profile 1.1 should not be confused with SAML version 1.1. SAML version 1.1 is **not** used by the Nationwide Health Information Network; the NHIN specifications are based on SAML version 2.0.)

2.4.1 Processing Model

As per section 3.1 in:
http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf

This specification extends the token-independent processing model defined by the WSS: SOAP Message Security specification.

When a receiver processes a <wsse:Security> header containing or referencing SAML assertions, it selects, based on its policy, the signatures and assertions that it will process. It is assumed that a receiver's signature selection policy MAY rely on semantic labeling of <wsse:SecurityTokenReference> elements occurring in the <ds:KeyInfo> elements within the signatures. It is also assumed that the assertions selected for validation and processing will include those referenced from the <ds:KeyInfo> and <ds:SignedInfo> elements of the selected signatures.

As part of its validation and processing of the selected assertions, the receiver MUST establish the relationship between the subject and claims of the SAML statements (of the referenced SAML assertions) and the entity providing the evidence to satisfy the confirmation method defined for the statements (i.e., the attesting entity). Two methods for establishing this correspondence, holder-of-key and sender-vouches are described below. Systems implementing this specification MUST implement the processing necessary to support both of these subject confirmation methods

When the confirmation method is urn:oasis:names:tc:SAML:1.0:cm:bearer, proof of the relationship between the attesting entity and the subject of the statements in the assertion is implicit and no steps need be taken by the receiver to establish this relationship.

2.4.2 Terminology

http://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf

This specification employs the terminology defined in the WSS: SOAP Message Security specification. The definitions for additional terminology used in this specification appear below.

Attesting Entity – the entity that provides the confirmation evidence that will be used to establish the correspondence between the subjects and claims of SAML statements (in SAML assertions) and SOAP message content.

Confirmation Method Identifier – the value within a SAML SubjectConfirmation element that identifies the subject confirmation process to be used with the corresponding statements.

Subject Confirmation – the process of establishing the correspondence between the subject and claims of SAML statements (in SAML assertions) and SOAP message content by verifying the confirmation evidence provided by an attesting entity.

SAML Assertion Authority - A system entity that issues assertions.

Subject – A representation of the entity to which the claims in one or more SAML statements apply

3 Framework Definition

3.1 Interaction Behavior

According to the Nationwide Health Information Network's local accountability principle, the initiating NHIO must determine if a local user is authorized to perform a given function; in this context, to make a specific request. If the request is authorized, the initiating NHIO attaches the user-centric assertions to the request.

The responding NHIO receives the request with the understanding that the initiating NHIO has locally authorized the user to make the request. However, according to the local autonomy principle, the decision to grant the request is that of the responding NHIO. The information needed to inform that decision is conveyed via SAML assertions.

Figure 3.1-1 Interaction Behavior

The responding NHIO receives the request with assertions and consults a local Policy Authority or Policy Enforcement Point (which could be a SAML authority) to establish whether it should perform the function. Assertions can convey information about methods used to authenticate the user, user attributes, and authorization decisions about whether users are allowed to access certain resources. A single assertion may contain several different internal statements about authentication, authorization, and attributes.[2]

[2] SAML v2.0

Specific Nationwide Health Information Network Assertions

The following set of SAML assertions are designated as required or optional for all communications between NHIOs.[3]

Figure 3.2-1: Non-Normative example of the position of the SAML Assertion within the SOAP Header

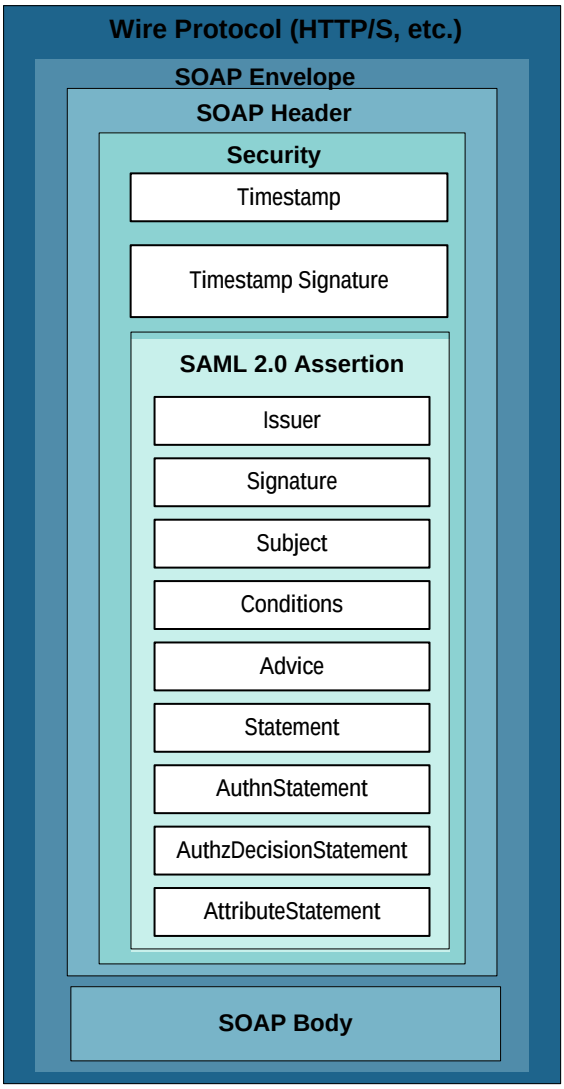

Figure 3.2-1 depicts how the SAML header adopted here is carried within the <Security> element within the header of the SOAP envelope as defined by WS-Security. The Nationwide Health Information Network does not constrain SAML other than as defined by underlying specifications. The ordering of the elements with the SAML 2.0 security header is normatively defined by the underlying SAML 2.0 schemas and specifications.

[3] See section 1.4, OASIS Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)

3.1.1 Namespaces

Table 3.2.1-1 Common Namespaces used in SOAP Message Security

Prefix	Namespace
ds	http://www.w3.org/2000/09/xmldsig#
S11	http://schemas.xmlsoap.org/soap/envelope/
S12	http://www.w3.org/2003/05/soap-envelope
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
wsse11	http://docs.oasis-open.org/wss/oasis-wss-wssecurity-secext-1.1.xsd
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd
xenc	http://www.w3.org/2001/04/xmlenc#

3.1.2 Timestamp

Each Nationwide Health Information Network Request shall have a <wsse:Security> element which contains the entire SAML token. This is per the Web Services Security: SAML Token Profile 1.1 specification. Also as per the spec the <wsse:SecurityTokenReference> tags should also be present after the saml:Assertion.
The <wsse:Security> element will contain a <wsu:Timestamp> element to provide the ability to express the creation and expiration times of the message. The ID attribute provides the ability to reference this timestamp in an XML Signature. The <wsu:Timestamp> element will contain both a <wsu:Created> and an <wsu:Expires> element to express the temporal security semantics. All times must be in UTC format as specified by the XML Schema type (dateTime). The ordering of the elements must have <wsu:Created> followed by <wsu:Expires>. The following illustrates the syntax of this element:

Figure 3.2.2-1 Timestamp Element Example

```
<wsu:Timestamp wsu:Id="_1">
  <wsu:Created>2008-10-07T13:00:34Z</wsu:Created>
  <wsu:Expires>2008-10-07T13:05:34Z</wsu:Expires>
</wsu:Timestamp>
```

In order to prevent the manipulation of the stated range of valid times for the given message by a third party in a replay attack, the security timestamp is digitally signed. The <wsse:Security> element will contain a <ds:Signature> element which specifies the algorithms and transformations applied during the signing process. This element must conform to the XML Signature specification, which is described in section 3.3.4. However, in this case, enclosed within the <ds:KeyInfo> element of the <ds:Signature> is the <wsse:SecurityTokenReference> element. This element provides the ability to reference the SAML Assertion.

Referencing Section 3.4 in the OASIS WSS SAML Token Profile 1.1 standard, as per Table-2 Key Identifier ValueType Attribute Values, and Table-3 TokenType Attribute Values: The wsse11:TokenType attribute is used to declare the type of the referenced token for SAML v2.0. This is defined to be: http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0. The <wsse:KeyIdentifier> has a ValueType attribute which defines the type of value contained in this element. For SAML v2.0 this is defined to be: http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID. The value contained will reference the SAML Assertion's identifier. The following illustrates the syntax of this element:

Figure 3.2.2-2 KeyInfo Element Example

```
<ds:KeyInfo>
  <wsse:SecurityTokenReference  wsu:Id="uuid_2ca69267-90bd-4785-a28e-ad9cee6d962e"
    wsse11:TokenType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0">
    <wsse:KeyIdentifier
 ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID"
```

```
    >ed62b6fb-4d73-4011-9f7c-43e0575b6317</wsse:KeyIdentifier>
  </wsse:SecurityTokenReference>
</ds:KeyInfo>
```

In addition to the Security element timestamp signature described in this section, the SAML Assertion must also be digitally signed as described in Section 3.3.4 of this specification.

3.2 SAML Assertions

Each Nationwide Health Information Network Request shall have a saml:Assertion element containing child elements saml:Issuer, saml:Subject, saml:AuthnStatement, and saml:AttributeStatement. (No saml:Assertion element is required on a response to a Nationwide Health Information Network Request.) The use of saml:AuthorizationDecisionStatement is optional.

Normative: An NHIN Initiating Gateway MUST use a SAML 2.0 assertion in the security header of SOAP messages, with at least the requirements as defined in section 3.3 of this specification, with at least one "holder-of-key" subject confirmation method. An NHIN Responding Gateway MUST have the capability to process the SAML 2.0 holder-of-key assertions, employing a processing model as per the OASIS SAML 2.0 "Processing Model" specifications and as per the NHIN specifications. In addition to a single required holder-of-key subject confirmation method, other SAML 2.0 subject confirmation methods MAY be used. The NHIN Initiating Gateway MAY supply more than one subject confirmation method, and those methods MAY include additional holder-of-key subject confirmation methods, and they MAY include one or more "sender-vouches" subject confirmation methods, and they MAY include one or more "bearer" subject confirmation methods. The use of more than a single holder-of-key subject confirmation method is not defined in this specification, but should be defined by higher-level profiles, specifications, or private business agreements between the NHIN Initiating Gateway and the NHIN Responding Gateway.

Non-normative: The requirement to supply at least one holder-of-key subject confirmation method is intended to a) ensure interoperability by establishing a singular security base approach; b) ensure interoperability with NHIN gateways existing prior to the publication of this version of this specification (backwards compatibility); c) NOT intended to be the only subject confirmation method allowed in the future. When, and if, an approved use case exists that requires the NHIN Authorization Framework specified use of alternate subject confirmation methods, the authoring team intends to update this specification accordingly.

Normative: The 2-way-TLS mutual authentication, covered elsewhere, MUST employ an ONC-managed Certification Authority issued certificate. The x.509 certificate used by the Authorization Framework to sign the <Timestamp> and <saml> apexes of the SOAP message MUST also be issued by the ONC-managed Certification Authority (CA).

Non-normative: Operationally, as per experience to date, the certificate used to establish the 2-way-TLS mutual gateway authentication should be the same as the certificate used to sign <timestamp> and <SAML> apexes of the SOAP message. It is anticipated that these certificates will be different, and participants are advised to build their systems to accept different certificates for the 2-way-TLS purposes and the SOAP message signatures in the future.

SAML Assertions must include:

1. Version attribute which defines SAML v2.0 as the version

2. ID attribute which is an xs:ID as defined by http://www.w3.org/TR/xml-id/

   Normative: The Nationwide Health Information Network doesn't constrain the value of the assertion ID; it is only constrained by the underlying SAML and W3C specifications.

   Non-normative: Prior examples in this specification documented the assertion ID in a technically correct manner, but were unintentionally misleading.. Specifically, the prior examples used a UUID, but the underlying specifications identify this is a W3C ID type. This resulted in some prior implementers assuming this identifier could be a UUID, which was incorrect as the assertion ID must not start with a number. Implementers are advised to treat this as an opaque data type.

Based on evidence, implementers SHOULD construct this identifier by prepending an underscore character ("_") to a UUID value.

The following illustrates the syntax of this element:

Figure 3.3-1 Assertion ID Element Example

```
<saml2:Assertion ID="_ed62b6fb-4d73-4011-9f7c-43e0575b6317"
         IssueInstant="2008-10-07T13:00:34.484Z" Version="2.0">
```

3. IssueInstant attribute which is an xs:dateTime as defined by http://www.w3.org/TR/xmlschema-2/

4. Normative: The <Issuer> element is not constrained by this specification.

   Non-normative: The Nationwide Health Information Network, as of the time this text was written, has issued no policy or specification constraining the <Issuer> element; it is only constrained by the underlying OASIS SAML 2.0 specifications, referenced elsewhere in this document. As per SAML, the <Issuer> MUST specify the SAML authority that is making the claim(s) in the assertion. The issuer SHOULD be unambiguous to the intended relying parties. In the absence of policy to the contrary, and based on historical evidence, implementers should use a name NameIDType Format of "x.509 Subject Name" type as specified in 8.3.3 of the OASIS SAML 2.0 core specification. Use of "8.3.1 Unspecified" as a NameIDType Format is not recommended.

5. The <Subject> element shall identify the Subject[4] of the assertion. This element also includes a NameID Format attribute, which declares the format used to express the value contained in this element – the person making the request at the initiating NHIO. SAML 2.0 NameID Formats are provided in Table 3.3-1 of this specification, however only formats “X509SubjectName” and “emailAddress” are allowed in this element. For further explanation of the other elements and attributes contained in the <Subject> element, refer to the SAML 2.0 standard as referenced in section 1.4 of this specification.

The following is an example of the <Subject> element:

Figure 3.3-2 Subject Element Example

```
<Subject>
  <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
    CN=Alex G. Bell,O=1.22.333.4444,UID=abell
  </NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:holder-of-key">
    <SubjectConfirmationData>
      <ds:KeyInfo>
        <ds:KeyValue>
          <ds:RSAKeyValue>
            <ds:Modulus>vYxVZKIzVdGMSBkW4bYnV80MV/RgQKV1bf/DX8laMO45P6uYp+snzz2XM0S6o3JGQtXQ=
            </ds:Modulus>
            <ds:Exponent>AQAB</ds:Exponent>
          </ds:RSAKeyValue>
        </ds:KeyValue>
      </ds:KeyInfo>
    </SubjectConfirmationData>
  </SubjectConfirmation>
</Subject>
```

[4] Note that the term “subject” in SAML and XACML refers to the individual making the request. In this specification, the term “User” is generally used with the same meaning, but when referring to attributes defined in SAML or XACML, the naming convention of the standard is retained.

Table 3.3-1 NameID Format URIs

Format	URI
Unspecified	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Email Address	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
X.509	urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
Windows	urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName
Kerberos	urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos
Entity	urn:oasis:names:tc:SAML:2.0:nameid-format:entity
Persistent	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
Transient	urn:oasis:names:tc:SAML:2.0:nameid-format:transient

6. SAML Statement Elements - The SAML statement elements used are separated into Authentication, Attribute, and Authorization Decision statements. Each statement will be further defined in the following paragraphs.

3.2.1 Authentication Statement

The authentication assertions are associated with authentication of the Subject (User). The <AuthnStatement> element is required to contain an <AuthnContext> element and an AuthnInstant attribute. The saml:AuthnStatement shall contain one saml:AuthnContextClassRef element identifying the method by which the subject was authenticated. Other optional elements of saml:AuthnStatement may also be included, such as a <SubjectLocality> element and a SessionIndex attribute. Each of these is described in more detail in the sections that follow.

The saml:Authentication is comprised of the following 4 Attributes or Elements:

1. AuthnContext
2. Subject Locality (Optional)
3. AuthnInstant
4. Session Index (Optional)

3.2.1.1 Authentication method

The <AuthnContext> element (required) indicates how that authentication was done. Note that the authentication statement does not provide the means to perform that authentication, such as a password, key, or certificate. This element will contain an authentication context class reference.[5]
Available authentication methods and their corresponding URNs are provided in the following table:

Table 1.3.1-1 Authentication Methods

Authentication Method	URN
Internet Protocol	urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
Internet Protocol Password	urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocolPassword
Password	urn:oasis:names:tc:SAML:2.0:ac:classes:Password
Password Protected Transport	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Kerberos	urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
Previous Session	urn:oasis:names:tc:SAML:2.0:ac:classes:PreviousSession

[5] Refer to section 1.4, OASIS: Authentication Context for Security Assertion Markup Language (SAML) for more information

Secure Remote Password	urn:oasis:names:tc:SAML:2.0:ac:classes:SecureRemotePassword
SSL/TLS Certificate	urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient
X.509 Public Key	urn:oasis:names:tc:SAML:2.0:ac:classes:X509
PGP Public Key	urn:oasis:names:tc:SAML:2.0:ac:classes:PGP
SPKI Public Key	urn:oasis:names:tc:SAML:2.0:ac:classes:SPKI
XML Digital Signature	urn:oasis:names:tc:SAML:2.0:ac:classes:XMLDSig
Unspecified	urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified

3.2.1.2 Subject Locality from Where the User was Authenticated

The <SubjectLocality> element (optional) specifies the DNS domain name and IP address for the system entity that was authenticated.

3.2.1.3 Authentication Instant

The AuthnInstant attribute (required) specifies the time at which the authentication took place.

3.2.1.4 Session Index

The SessionIndex attribute (optional) identifies the session between the Subject and the Authentication Authority.

Figure 3.3.1-1 Authentication Example

```
<saml:AuthnStatement AuthnInstant="2005-01-31T12:00:00Z" SessionIndex="67775277772">
  <saml:SubjectLocality Address="112.16.133.144" DNSName="ME001122.csrk.mynetwork.net"/>
  <saml:AuthnContext>
    <saml:AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>
```

3.2.2 Attribute Statement

The <AttributeStatement> element describes a statement by the SAML authority asserting that the requesting user is associated with the specified attributes. The <AttributeStatement> is required to contain <Attribute> elements as defined by the OASIS XSPA profile of SAML and described in the sections that follow.

The NHIN defines the use of the following 8 attributes in the saml:AttributeStatement (use of additional attributes is allowed, but not defined, by this specification):

1. Subject ID
2. Subject Organization
3. Subject Role
4. Purpose Of Use
5. Home Community ID
6. Organization ID
7. Resource ID (Optional)
8. National Provider Identifier (Optional)

The value on the Subject ID and Subject Organization attributes shall be a plain text description of the user's name (not user ID) and organization, respectively. These are primarily intended to support auditing.

3.2.2.1 Subject ID Attribute

This <Attribute> element shall have the Name attribute set to "urn:oasis:names:tc:xspa:1.0:subject:subject-id". The name of the user as required by HIPAA Privacy Disclosure Accounting shall be placed in the value of the <AttributeValue> element. (Keep in mind that the term "subject" in SAML and XACML refers to the individual making the request; in this specification, the term "User" is generally used with the same meaning, but when referring to attributes defined in SAML or XACML, the naming convention of the standard is retained.)

The Nationwide Health Information Network uses the XSPA namespace for subject-id attribute. The primary purpose of this identifier is for display and logging. This XSPA identifier should not be confused with the subject-id identifier from the XACML namespace identifier which is intended for a different purpose.

An example of the syntax of this element is as follows:

Figure 3.3.2.1-1 Subject ID Attribute Example

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
  <saml:AttributeValue>Walter H.Brattain IV</saml:AttributeValue>
</saml:Attribute>
```

The Nationwide Health Information Network Trial Implementation "UserName" attribute has been replaced by the Subject ID attribute defined in this section.

3.2.2.2 Subject Organization Attribute

This <Attribute> element shall have the Name attribute set to "urn:oasis:names:tc:xspa:1.0:subject:organization". In plain text, the organization that the user belongs to as required by HIPAA Privacy Disclosure Accounting shall be placed in the value of the <AttributeValue> element.

An example of the syntax of this element is as follows:

Figure 3.3.2.2-1 Subject Organization Attribute Example

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization">
  <saml:AttributeValue>Family Medical Clinic</saml:AttributeValue>
</saml:Attribute>
```

The Nationwide Health Information Network Trial Implementation "UserOrganization" attribute has been replaced by the Subject Organization attribute defined in this section.

3.2.2.3 Subject Organization ID Attribute

This <Attribute> element shall have the Name attribute set to "urn:oasis:names:tc:xspa:1.0:subject:organization-id" A unique identifier for the organization that the user is representing in performing this transaction shall be placed in the value of the <AttributeValue> element. This organization ID shall be consistent with the plain-text name of the organization provided in the User Organization Attribute. The organization ID may be an Object Identifier (OID), using the urn format (that is, "urn:oid:" appended with the OID); or it may be a URL assigned to that organization.

An example of the syntax of this element is as follows:

Figure 3.3.2.3-1 Subject Organization ID Attribute Example

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
  <saml:AttributeValue>http://familymedicalclinic.org</saml:AttributeValue>
</saml:Attribute>
```

3.2.2.4 Home Community ID Attribute

This <Attribute> element shall have the Name attribute set to “urn:nhin:names:saml:homeCommunityId”. The value shall be the Home Community ID (an Object Identifier) assigned to the NHIO that is initiating the request, using the urn format (that is, “urn:oid:” appended with the OID). For information regarding OIDs, refer to http://www.oid-info.com/faq.htm

An example of the syntax of this element is as follows:

Figure 3.3.2.4-1 Home Community ID Attribute Example

```
<saml:Attribute Name="urn:nhin:names:saml:homeCommunityId">
  <saml:AttributeValue>urn:oid:2.16.840.1.113883.3.190</saml:AttributeValue>
</saml:Attribute>
```

3.2.2.5 Role Attribute

This <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xacml:2.0:subject:role”. The value of the <AttributeValue> element is a child element, “Role”, in the namespace “urn:hl7-org:v3”, whose content is defined by the “CE” (coded element) data type from the HL7 version 3 specification.

The codeSystem is defined to be “2.16.840.1.113883.6.96" and the codeSystemName is defined to be "SNOMED_CT". The Role Element shall contain the SNOMED CT value representing the role that the user is playing when making the request. The value set to be used is “User Role” and the OID 2.16.840.1.113883.3.18.6.1.15[6] as defined in HITSP C80.

An example of the syntax of this element is as follows:

Figure 3.3.2.5-1 Role Attribute Example

```
<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
  <saml:AttributeValue>
    <Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="46255001"
       codeSystem="2.16.840.1.113883.6.96" codeSystemName="SNOMED_CT"
       displayName="Pharmacist"/>
  </saml:AttributeValue>
</saml:Attribute>
```

The Nationwide Health Information Network Trial Implementation “UserRole” attribute has been replaced by the Subject Role attribute defined in this section.

3.2.2.6 Purpose Of Use Attribute

This <Attribute> element shall have the Name attribute set to “urn:oasis:names:tc:xspa:1.0:subject:purposeofuse”[7]. The value of the <AttributeValue> element is a child element, “PurposeOfUse”, in the namespace “urn:hl7-org:v3”, whose content is defined by the “CE” (coded element) data type from the HL7 version 3 specification.

The PurposeOfUse element shall contain the coded representation of the reason for the request.

An example of the syntax of this element is as follows:

[6] At this time, it is not anticipated that this value set OID is required for any particular purpose, but it is defined as a vocabulary best practice.

[7] Readers of the XSPA Profile of SAML referenced in section 3.3.2 of this specification may note that the Conformance Table shows xspa:1,0 rather than xspa:1.0. NHIN believes this to be a typo and has specified the use of a decimal rather than a comma.

Figure 3.3.2.6-1 PurposeOfUse Attribute Example

```
<saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
  <saml:AttributeValue>
    <PurposeOfUse xmlns="urn:hl7-org:v3" xsi:type="CE" code="OPERATIONS"
        codeSystem="2.16.840.1.113883.3.18.7.1" codeSystemName="nhin-purpose"
        displayName="Healthcare Operations"/>
  </saml:AttributeValue>
</saml:Attribute>
```

Non-normative implementation note: CAUTION: As of September, 2010, the Nationwide Health Information Network Exchange has become aware of a potentially breaking change related to the SAML 2.0 PurposeOfUse AttributeValue.

In prior versions of this specification, in the immediately prior non-normative example, the example text was incorrect and inconsistent with the remaining text in this document. Specifically, the example text stated “PurposeForUse” instead of the correct “PurposeOfUse”. The incorrect PurposeForUse attribute has been implemented by some Nationwide Health Information Network Exchange members and thus future implementers are cautioned to be aware of this potential interoperability issue.

For more detailed and more recent information on this topic, please see the Nationwide Health Information Network Exchange’s Wiki page at: http://exchange-specifications.wikispaces.com/Auth+PurposeOfUse+Research or the main Security and Privacy Workgroup page at: http://exchange-specifications.wikispaces.com/Security+and+Privacy+Team .

Codes are assigned as below. The codeSystem is defined to be “2.16.840.1.113883.3.18.7.1”. The codeSystemName is defined to be “nhin-purpose”. The value of the PurposeOfUse attribute shall be an urn:hl7-org:v3:CE element, specifying the coded value representing the user's purpose in issuing the request, choosing from the value set listed in this specification. The codeSystem attribute of this element must be present, and must specify the OID of the "PurposeOfUse" code system created by the Nationwide Health Information Network Cooperative, 2.16.840.1.113883.3.18.7.1 .

The value set for Purpose Of Use is defined in Table 3.3.2.6-1, below.

Table 3.3.2.6-1 Nationwide Health Information Network PurposeOfUse Code Description

PurposeOfUse vocabulary	Code
Treatment	TREATMENT
Payment	PAYMENT
Healthcare Operations	OPERATIONS
System Administration	SYSADMIN
Fraud detection	FRAUD
Use or disclosure of Psychotherapy Notes	PSYCHOTHERAPY
Use or disclosure by the covered entity for its own training programs	TRAINING
Use or disclosure by the covered entity to defend itself in a legal action	LEGAL
Marketing	MARKETING
Use and disclosure for facility directories	DIRECTORY
Disclose to a family member, other relative, or a close personal friend of the individual,	FAMILY
Uses and disclosures with the individual present.	PRESENT
Permission cannot practicably be provided because of the individual’s incapacity or an emergency	EMERGENCY
Use and disclosures for disaster relief purposes.	DISASTER

Uses and disclosures for public health activities.	PUBLICHEALTH
Disclosures about victims of abuse, neglect or domestic violence.	ABUSE
Uses and disclosures for health oversight activities.	OVERSIGHT
Disclosures for judicial and administrative proceedings.	JUDICIAL
Disclosures for law enforcement purposes.	LAW
Uses and disclosures about decedents.	DECEASED
Uses and disclosures for cadaveric organ, eye or tissue donation purposes	DONATION
Uses and disclosures for research purposes.	RESEARCH
Uses and disclosures to avert a serious threat to health or safety.	THREAT
Uses and disclosures for specialized government functions.	GOVERNMENT
Disclosures for workers' compensation.	WORKERSCOMP
Disclosures for insurance or disability coverage determination	COVERAGE
Request of the Individual	REQUEST

3.2.2.7 Patient Identifier Attribute

This attribute is OPTIONAL, as it may not be needed for cases in which the data being exchanged does not pertain to a specific patient (e.g. population health data). The value of the Patient Identifier attribute MUST be specified when the InstanceAccessConsentPolicy attribute is specified in an Authorization Decision Statement.

This <Attribute> element shall have the Name attribute set to "urn:oasis:names:tc:xacml:2.0:resource:resource-id". The patient identifier of the requesting organization shall be placed in the value of the <AttributeValue> element.

Note to implementers: there is a known issue related to the version of the above identifier, specifically the text "2.0" appears to be used inconsistently in the underlying specifications (in some instances "2.0" is used and other instances it is "1.0" is used). The NHIN has elected to use the "urn:oasis:names:tc:xacml:2.0:resource:resource-id" as opposed to "urn:oasis:names:tc:xacml:1.0:resource:resource-id" at this time. In the future this may change and implementers are guided to be aware of this potential issue.

The patient identifier MUST consist of two parts; the OID for the assigning authority and the identifier of the patient within that assigning authority. The value MUST be formatted using the following syntax:

IDNumber^^^&OIDofAA&ISO

where IDNumber is the identifier of the patient within the assigning authority, and OIDofAA is the OID for the assigning authority. As an example, a patient identifier of 543797436 for an assigning authority with an OID of 1.2.840.113619.6.197, has been encoded into the follow SAML assertion snippet. Please note that the '&' character has been properly encoded in the XML content.

Figure 3.3.2.7-1 Patient Identifier Attribute Example

```
<saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
  <saml:AttributeValue>543797436^^^&amp;1.2.840.113619.6.197&amp;ISO</saml:AttributeValue>
</saml:Attribute>
```

3.2.2.8 National Provider Identifier (NPI) Attribute

A National Provider Identifier (NPI) is a unique 10-digit identification number issued to health care providers in the United States by the Centers for Medicare and Medicaid Services (CMS). This attribute

provides the ability to specify an NPI value as part of the SAML assertion that accompanies a message that is transmitted across the Nationwide Health Information Network.

The NPI attribute is OPTIONAL, and is therefore, NOT required for ALL Nationwide Health Information Network messages. When this attribute is included in the SAML assertion, the <Attribute> element SHALL have the Name attribute set to “urn:oasis:names:tc:xspa:2.0:subject:npi”. An example of the syntax of this element follows:

Figure 3.3.2.8-1 National Provider Identifier Attribute Example

```
<saml:Attribute Name=" urn:oasis:names:tc:xspa:2.0:subject:npi">
  <saml:AttributeValue>1234567890</saml:AttributeValue>
</saml:Attribute>
```

3.2.2.9 Attribute Statement Example

Please see section 3.3.2.6 for guidance regarding the PurposeOfUse attribute.

Figure 3.3.2.9-1 Attribute Statement Example

```
<saml:AttributeStatement>
  <saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:subject-id">
    <saml:AttributeValue>Dr Joe Smith</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization">
    <saml:AttributeValue>Best Clinic</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:organization-id">
    <saml:AttributeValue>urn:oid: 2.16.840.1.113883.3.18.101</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:nhin:names:saml:homeCommunityId">
    <saml:AttributeValue>urn:oid:2.16.840.1.113883.3.190</saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:subject:role">
    <saml:AttributeValue>
      <Role xmlns="urn:hl7-org:v3" xsi:type="CE" code="112247003"
         codeSystem="2.16.840.1.113883.6.96"
         codeSystemName="SNOMED CT" displayName="Medical doctor"/>
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:oasis:names:tc:xspa:1.0:subject:purposeofuse">
    <saml:AttributeValue>
      <PurposeOfUse xmlns="urn:hl7-org:v3" xsi:type="CE" code="TREATMENT"
         codeSystem="2.16.840.1.113883.3.18.7.1"
        codeSystemName="nhin-purpose" displayName="Treatment"/>
    </saml:AttributeValue>
  </saml:Attribute>

  <saml:Attribute Name="urn:oasis:names:tc:xacml:2.0:resource:resource-id">
    <saml:AttributeValue>543797436^^^&amp;1.2.840.113619.6.197&amp;ISO</saml:AttributeValue>
  </saml:Attribute>

</saml:AttributeStatement>
```

3.2.3 Authorization Decision Statement

The <AuthzDecisionStatement> element describes a statement by the SAML authority asserting that a request for access by the statement's subject to the specified resource has resulted in the specified authorization decision based on some optionally specified evidence. This OPTIONAL element provides the requesting NHIO an opportunity to assert that it holds an Access Consent Policy, which the responding Nationwide Health Information Network may wish to evaluate in order to determine if access to the requested resource(s) should be allowed.
The information conveyed within the Authorization Decision Statement may be used by the responding NHIO to retrieve the asserted Access Consent Policy. The format of the Access Consent Policy is defined in the Nationwide Health Information Network Access Consent Policy specification.

The Authorization Decision Statement WILL be used when the consumer (patient) has granted the requesting NHIO permission to access to their medical records, and the requester needs to make that authorization known to another (responding) NHIO.

The underlying assumption for this use case is that the responding NHIO has medical records for the consumer, but has access restrictions in place that would ordinarily prevent disclosure of the patient's records to the requesting NHIO. A variation of this use case is that the responding NHIO's policies or access restrictions would prevent disclosure of the patient's identity to the requesting NHIO through the Nationwide Health Information Network Patient Discovery mechanism, effectively preventing the requesting NHIO from making a query and subsequent request for medical records.

3.2.3.1 Authorization Decision Statement Content

The Authorization Decision Statement has the following content:

1. Action. This action must be specified using a Namespace of 'urn:oasis:names:tc:SAML:1.0:action:rwedc' and a value of Execute.[8]
2. Decision. The Decision attribute of the Authorization Decision Statement must be "Permit".
3. Resource. The Resource attribute of the Authorization Decision Statement must be the URI of the endpoint to which the request is addressed or an empty URI reference ("").
4. The Authorization Decision Statement must contain an <Evidence> element, containing a single <Assertion> child element.
5. This <Assertion> element must contain an ID attribute, an IssueInstant attribute, a Version attribute, an Issuer element, and an Attribute Statement element.
6. There must be at least one of the following Attributes in the Attribute Statement.
    1. An <Attribute> element with the name "AccessConsentPolicy" and NameFormat "http://www.hhs.gov/healthit/nhin". The value(s) for this attribute will be the OIDs of the access policies that the asserting entity has previously agreed to with other entities. The OIDs MUST be expressed using the urn format (e.g. - urn:oid:1.2.3.4).
    2. An <Attribute> element with the name "InstanceAccessConsentPolicy" and NameFormat "http://www.hhs.gov/healthit/nhin". The value(s) of this attribute will be the OIDs of the

[8] This document was updated to specify this namespace prior to publication, but after the previous namespace had been incorporated in Connect 2.3. There will be a short period of time where the namespace used in the Connect Gateway does not conform to this spec.

patient specific access policy instances. The OIDs MUST be expressed using the urn format (e.g. - urn:oid:1.2.3.4.123456789). If a requester specifies this Attribute, the requestor MUST support the ability for the specified policy document(s) to be retrieved via the transactions defined in HITSP TP30.

3. The “ContentReference”, “ContentType”, and “Content” attributes from the Trial Implementation specifications have been removed and should no longer be used.

3.2.3.2 Authorization Decision Statement Example

See section 3.3, item 3 for information about this ID value.

Figure 3.3.3-1 Authorization Decision Statement Example

```
<saml2:AuthzDecisionStatement xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
     Decision="Permit"
     Resource="">
          <saml2:Action
           Namespace="urn:oasis:names:tc:SAML:1.0:action:rwedc">Execute</saml2:Action>
          <saml2:Evidence>
              <saml2:Assertion ID="_da20c267-0f95-4cf4-8bc1-6daa5d84201e"
                  IssueInstant="2008-10-20T19:59:10.843Z" Version="2.0">
                <saml2:Issuer Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
>CN=SAML User,OU=SU,O=SAML User,L=Los Angeles,ST=CA,C=US</saml2:Issuer>
                 <saml2:Conditions NotBefore="2008-10-20T19:59:10.843Z"
                                   NotOnOrAfter="2008-12-25T00:00:00.000Z"/>
               <saml2:AttributeStatement>
                    <saml2:Attribute Name="AccessConsentPolicy"
                        NameFormat="http://www.hhs.gov/healthit/nhin">
                       <saml2:AttributeValue>urn:oid:1.2.3.4</saml2:AttributeValue>
                    </saml2:Attribute>
                   <saml2:Attribute Name="InstanceAccessConsentPolicy"
                            NameFormat="http://www.hhs.gov/healthit/nhin">
                       <saml2:AttributeValue
                          xmlns:ns6="http://www.w3.org/2001/XMLSchema-instance"
                          xmlns:ns7="http://www.w3.org/2001/XMLSchema"
                          ns6:type="ns7:string">urn:oid:1.2.3.4.123456789
                       </saml2:AttributeValue>
                   </saml2:Attribute>
               </saml2:AttributeStatement>
             </saml2:Assertion>
        </saml2:Evidence>
</saml2:AuthzDecisionStatement>
```

3.2.4 Assertion Signature

An assertion signed by the asserting party supports assertion integrity, authentication of the asserting party to the receiving party, and, if the signature is based on the SAML authority’s public/private key pair, non-repudiation of origin. For Nationwide Health Information Network purposes the <ds:Signature> element is required to contain a <ds:SignedInfo> element , a <ds:SignatureValue> element, and a <ds:KeyInfo> element.

3.2.4.1 SignedInfo Element

The <ds:SignedInfo> element is a container which specifies the <ds:CanonicalizationMethod>, the <ds:SignatureMethod>, and a <ds:Reference>.

Normative: Exclusive Canonicalization MUST be used for SAML 2.0 Assertion XML-Digital Signatures as specified by the W3CExclusive XML Canonicalization Version 1.0 specification.

Non-normative: Use of Exclusive Canonicalization ensures that signatures created for any sub-document (apex) of an XML document can be verified independently of the context. This capability is important to ensure that the substantive content of an XML sub-document can be validated as being unmodified even

if that sub-document is moved into a new document, or moved in relation to other content in the same document. One anticipated use of this capability is to allow intermediaries to add additional signatures or XML wrappers. Although other canonicalization methods are allowed by the underlying specifications, the Nationwide Health Information Network requires the use of Exclusive Canonicalization due to security vulnerabilities potentially exposed by other canonicalization methods.

The <ds:SignatureMethod> identifies the cryptographic functions involved in the signature operation. It is recommended that SAML processors support the use of RSA signing and verification, http://www.w3.org/2000/09/xmldsig#rsa-sha1.

XML Digital Signatures are applied to data objects through an indirection or URI reference; when signing the SAML assertion the URI reference must match the Assertion ID attribute value. The <ds:Reference> element also specifies the transformation algorithms the digest method and the calculated digest value.

The transformation algorithms must be listed in the order that they are to be applied and may only consist of a subset of enveloped signature transform, exclusive canonicalization transform, and exclusive canonicalization with comments.

http://www.w3.org/2000/09/xmldsig#enveloped-signature http://www.w3.org/2001/10/xml-exc-c14n# http://www.w3.org/2001/10/xml-exc-c14n#WithComments

The <ds:DigestMethod> defines the digest algorithm that is applied. For the NHIN the Basic128 Algorithm Suite has been designated; such that the digest algorithm is defined to be SHA1; http://www.w3.org/2000/09/xmldsig#sha1.

3.2.4.2 SignatureValue Element

The SignatureValue element contains the actual value of the digital signature; it is always encoded using base64. The procedure to generate the digital signature is as stated below:

1) Identify the Assertion object to be signed
2) Apply the transformations provided in the <ds:Transformations> element to the Assertion object in the order as specified.
3) Apply the digest method which will result in generating the digest value
4) Create the <ds:Reference> element using the URI reference to the Assertion object and by enclosing the transformations, the digest method, and the calculated value.
5) Create the <ds:SignedInfo> element by enclosing the Canonicalization method, the Signature method, and the Reference as created above.
6) Apply the Canonicalization method to the created <ds:SignedInfo> element.
7) Apply the Signature method to generate the Signature value.

3.2.4.3 KeyInfo Element

The <ds:KeyInfo> element provides the means by which the signature is validated. This element must contain a <ds:KeyValue> element which contains a single public key that will be used to validate the signature. The enclosed <ds:RSAKeyValue> element identifies the structured format of the Nationwide Health Information Network provided keys to be RSA. This element declares the modulus, which applies to both the public and the private key, and the public key exponent. Each private key exponent is determined by a congruence relationship with the public key exponent and is known only to the party

generating the signature. These arbitrary-length integers are represented in XML as octet strings as defined by the ds:CryptoBinary type, which is a base64Binary

3.2.4.4 Signature Example

Figure 3.3.4.4-1 Signature Example

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="#51cb7689-0957-46a2-938e-1add75577ab7">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>a3XVN23H2N/ga+08AGqGHD1euKc=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>L8Liyz+6pLwNP9YBfIRbrDVUJtM2YcLuN3+HPjspQEHmZ2uTXWYuy7XTM9dqmN93w0ypVM7egjRe
=</ds:SignatureValue>
  <ds:KeyInfo>
    <ds:KeyValue>
      <ds:RSAKeyValue>
        <ds:Modulus>vYxVZKIzVdGMSBkW4bYnV80MV/RgQKV1bf/DoMTX8laMO45P6=</ds:Modulus>
        <ds:Exponent>AQAB</ds:Exponent>
      </ds:RSAKeyValue>
    </ds:KeyValue>
  </ds:KeyInfo>
</ds:Signature>
```

4 Error Handling

No additional faults are specified beyond the basic SOAP faults as identified in the Nationwide Health Information Network Messaging Platform Service Interface Specification.

5 Auditing

See each Nationwide Health Information Network service specification for specification-specific audit events.