Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML v2.0 for Healthcare Version 2.0

Committee Specification Draft 04 / Public Review Draft 04

25 February 2019

Specification URIs

This version:

https://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd04/saml-xspa-v2.0-csprd04.docx (Authoritative)
https://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd04/saml-xspa-v2.0-csprd04.html
https://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd04/saml-xspa-v2.0-csprd04.pdf

Previous version:

https://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd03/saml-xspa-v2.0-csprd03.docx (Authoritative)
https://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd03/saml-xspa-v2.0-csprd03.html
https://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd03/saml-xspa-v2.0-csprd03.pdf

Latest version:

https://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.docx (Authoritative)
https://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.html
https://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.pdf

Technical Committee:

OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) TC

Chairs:

Mohammad Jafari (mohammad.jafari@bookzurman.com), Veterans Health Administration
Christopher Shawn (christopher.shawn2@va.gov), Veterans Health Administration

Editors:

John M. Davis (mike.davis@va.gov), Veterans Health Administration
Duane DeCouteau (ddecouteau@edmondsci.com), Veterans Health Administration
Mohammad Jafari (mohammad.jafari@bookzurman.com), Veterans Health Administration

Related work:

This specification replaces or supersedes:

- *Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare Version 1.0*. Edited by Mike Davis, Duane DeCouteau and David Staggs. 1 November 2009. OASIS Standard. http://docs.oasis-open.org/security/xspa/v1.0/saml-xspa-1.0-os.html.

This specification is related to the OASIS Security Assertion Markup Language (SAML) V2.0, comprised of the following documents:

- *Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0*. Edited by John Kemp, Scott Cantor, Prateek Mishra, Rob Philpott, and Eve Maler.

15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf.

- *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. Edited by Scott Cantor, Frederick Hirsch, John Kemp, Rob Philpott, and Eve Maler. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf.
- *Conformance Requirements for the OASIS Security Assertion Mark Markup Language (SAML) V2.0*. Edited by Prateek Mishra, Rob Philpott, and Eve Maler. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf.
- *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. Edited by Scott Cantor, John Kemp, Rob Philpott, and Eve Maler. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.
- *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*. Edited by Jeff Hodges, Rob Philpott, and Eve Maler. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-glossary-2.0-os.pdf.
- *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. Edited by Scott Cantor, Jahan Moreh, Rob Philpott, and Eve Maler. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf.
- *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. Edited by John Hughes, Scott Cantor, Jeff Hodges, Frederick Hirsch, Prateek Mishra, Rob Philpott, and Eve Maler. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf.
- *Security Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0*. Edited by Frederick Hirsch, Rob Philpott, and Eve Maler. 15 March 2005. OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf.
- *SAML Version 2.0 Errata 05*. Edited by Scott Cantor. 01 May 2012. OASIS Approved Errata. http://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.html.

Declared XML namespaces:

- urn:oasis:names:tc:xspa:1.0
- urn:oasis:names:tc:xspa:2.0

Abstract:

This profile defines a set of SAML attributes and corresponding vocabularies for healthcare information exchange applications.

Status:

This document was last revised or approved by the OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) TC on the above date. The level of approval is also listed above. Check the “Latest version” location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xspa#technical.

TC members should send comments on this specification to the TC’s email list. Others should send comments to the TC’s public comment list, after subscribing to it by following the instructions at the “Send A Comment” button on the TC’s web page at https://www.oasis-open.org/committees/xspa/.

This specification is provided under the RF on Limited Terms Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/xspa/ipr.php).

Note that any machine-readable content (Computer Language Definitions) declared Normative for this Work Product is provided in separate plain text files. In the event of a

discrepancy between any such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

Citation format:

When referencing this specification the following citation format should be used:

[SAML-XSPA-v2.0]

Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of SAML v2.0 for Healthcare Version 2.0. Edited by John M. Davis, Duane DeCouteau, and Mohammad Jafari. 25 February 2019. OASIS Committee Specification Draft 04 / Public Review Draft 04. https://docs.oasis-open.org/xspa/saml-xspa/v2.0/csprd04/saml-xspa-v2.0-csprd04.html. Latest version: https://docs.oasis-open.org/xspa/saml-xspa/v2.0/saml-xspa-v2.0.html.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see https://www.oasis-open.org/policies-guidelines/trademark for above guidance.

Table of Contents

1 Introduction 7
1.1 IPR Policy 7
1.2 Terminology 7
1.3 Normative References 8
1.4 Non-Normative References 8
2 The XSPA Use-Cases 10
2.1 The Pull Use-Case 11
2.1.1 Variations 11
2.2 The Push Use-Case 11
2.3 The Trust Handshake Use-Case 12
2.4 Entities 12
2.4.1 Service Consumer Access Control Service 12
2.4.2 Service Provider Access Control Service 12
2.4.3 Security and Privacy Policies 13
2.4.4 Attributes 13
3 XSPA profile of SAML 14
3.1 Data Types 14
3.1.1 Concept Descriptor 14
3.1.1.1 Flattened Encoding 14
3.1.1.1.1 Example 14
3.1.1.2 Complex Attribute Encoding 15
3.1.1.2.1 Examples 15
3.2 Namespace Requirements 16
3.3 Attribute Naming Syntax, Restrictions and Acceptable Values 16
3.4 Attribute Rules of Equality 16
3.4.1 Attribute Identifiers 16
3.4.2 Attribute Values 16
3.5 Subject Identifier 16
3.6 Attributes 17
4 Other Considerations 19
4.1 Error States 19
4.1 Security Considerations 19
4.1.1 Transmission Security 19
4.2 Confirmation Identifiers 19
5 JSON Encoding 20
5.1 Attribute Identifiers 20
5.2 Attribute Values 21
5.2.1 Example 22
5.3 OpenID Connect Example 22
6 Conformance 23
6.1 US-Realm Conformance 23
Appendix A. Acknowledgments 25
Appendix B. Revision History 26

1 Introduction

This profile defines a set of SAML attributes and the corresponding vocabularies for healthcare information exchange applications.

1.1 IPR Policy

This specification is provided under the RF on Limited Terms Mode of the OASIS IPR Policy, the mode chosen when the Technical Committee was established. For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the TC's web page (https://www.oasis-open.org/committees/xspa/ipr.php).

1.2 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in **[RFC2119]**.

The following definitions establish additional terminology and usage in this profile:

Access Control Service (ACS)

A service that provides the basic operational aspects of access control such as making access control decision information (ADI) available to access decision components and performing access control functions **[HL7-SLS: Appendix A. Glossary of Terms]**. This service would be utilized by both the Service Provider and Service Consumer**.**

Functional Role

Functional roles are roles that are bound to the realization/performance of actions, such as *Authorizer*. **[ISO/TS 21298:2008: 5.5 Functional Roles]**.

Permission

An approval to perform an operation on one or more protected resources **[ANSI-INCITS 359-2004: 4. Terms and Definitions]**.

Principal

An entity whose identity can be authenticated. Examples include a human user, a process, a system, or an organization **[ITUT-X.811: 3.15. Principal]**.

Structural Role

Structural roles (also referred to as Organizational Roles) correspond to human or organizational categories and describe prerequisites, feasibilities, or competences for actions, for example *Dental Assistant*. Structural roles differ from policy domain to policy domain, within and across organizational boundaries, and especially between different jurisdictions and countries. **[ISO/TS 21298:2008: 5.3 Structural Roles]**.

Service Consumer (SC)

An individual entity, such as on an Electronic Health Record (EHR) or personal health record (PHR) System which makes a service request of a Service Provider.

Service Provider (SP)

A system, such as an Electronic Health Record System at a hospital, which provides protected resources and relies on the provided security service **[HL7-SLS: Appendix A. Glossary of Terms]**.

1.3 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[ANSI-INCITS 359-2004] ANSI-INCITS 359-2004 Role-Based Access Control. 2004.

[ASTM E1986-09(2013)] ASTM International, Standard Guide for Information Access Privileges to Health Information, DOI: 10.1520/E1986-09R13, 2013.

[SAML] "Security Assertion Markup Language (SAML) v2.0", OASIS Standard, 15 March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML-PROF] "Profiles for the OASIS Security Assertion Markup Language, v2.0," March 2005, OASIS Standard. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

[SAML-SUB-ID] "SAML V2.0 Subject Identifier Attributes Profile Version 1.0," September 2018, OASIS Committee Specification Draft. http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html

[HL7-HCS] HL7 Security Technical Committee, HL7 Healthcare Privacy and Security Classification System (HCS) Release 1, August 2014. http://www.hl7.org/implement/standards/product_brief.cfm?product_id=345

[ISO 21090:2011] International Organization for Standardization, ISO 21090, Health Informatics-- Harmonized Data Types for Information Interchange, 2011.

[ISO/TS 21298:2008] International Organization for Standardization, ISO/TS 21298, Health Informatics-- Functional and Structural Roles, 2008.

[HL7-PERM] HL7 Security Technical Committee, HL7 Version 3 Standard: Role-based Access Control Healthcare Permission Catalog, Release 2, February 2010. http://www.hl7.org/implement/standards/product_brief.cfm?product_id=72

[HL7-SLS] HL7 Version 3 Standard: Privacy, Access and Security Services Conceptual Model; Security Labeling Service, Release 1:2014. http://www.hl7.org/implement/standards/product_brief.cfm?product_id=360

[HL7-Vocab] HL7 Vocabulary Working Group, HL7 Vocabulary, Version: 1422-201812, December 2018.

[ITUT-X.811] ITU-T Recommendation X.811, Information Technology, Open Systems Interconnection, Security Framework for Open Systems, Authentication Framework, April 1995.

[NIST-800-63-1] National Institute of Standards and Technology, Special Publication 800-63-1, Electronic Authentication Guideline, December 2011. http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

[XACML-V3.0] eXtensible Access Control Markup Language (XACML) Version 3.0. 22 January 2013. OASIS Standard. http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

1.4 Non-Normative References

[HL7-Core-Schema-v3] HL7 International's Version 3 Normative Edition 2013, Processable Content, Core Schemas, ISO 21090 HL7 R2 Data Types, May 2013.

[HL7-FHIR] HL7**,** Fast Healthcare Interoperability Resources, STU; v3.0.1, April 2017, http://hl7.org/fhir

[NHIN-V3] Nationwide Health Information Network (NHIN), Authorization Framework, Version 3.0, July 2011. https://sequoiaproject.org/wp-

content/uploads/2014/11/nhin-authorization-framework-production-specification-v3.0.pdf

[OpenID-Connect] N. Sakimura, J. Bradley, et. al., OpenID Connect Core 1.0 incorporating errata set 1, https://openid.net/specs/openid-connect-core-1_0.html

[JSON] T. Bray, The JavaScript Object Notation (JSON) Data Interchange Format, https://tools.ietf.org/html/rfc7159

2 The XSPA Use-Cases

{non-normative}

The core use-cases for this profile are the cross-enterprise exchange of protected data objects from a Service Provider (SP) to a Service Consumer (SC) as depicted in Figure 1. Aside from this core use-case, there is also a use-case for establishing trust between two exchange partners as a precursor for future exchanges. Both of these use-cases and their variations, as well as the main entities and actors in Figure 1 will be discussed in the rest of this section.

There are a number of variations of the main exchange use-cases. In the Pull scenario, the SC sends a request to the SP asking for a data object (a Read command). In the Push Scenario, the SC sends a request to the SP which includes some data object to be accepted by the SP (a Create or Update command). In some cases, the request may include only a command and no data (a Delete or Execute command). The event flow for processing such requests is similar to that of Push. Another variation is the Publish/Subscribe use-case in which the SC sends a Subscription request and over time, receives a number of responses from SP.

In all of the above scenarios, the request includes SAML attribute assertions that vouch for the identity of the requesting Principal as well as other attribute consequential in making access control decisions at the SP's side. Some examples of such attributes are SC's organization identifier or the purpose of use for the transaction.

In the Pull and Subscription scenarios, these attributes are used by the SP's ACS to make the decision whether or not the requesting Principal is authorized to receive a copy of the requested data. In the Push scenario, these attributes are used by the SP's ACS to decide whether or not the requesting Principal is authorized to add new data to the SP, update existing data, or run a command such as Delete. These attributes may also vouch for the identity used to sign the submitted data object. The presented attributes are also used by the SP to record audit information about the transaction.

In the Pull and Subscription scenarios, the SP's response includes the requested data, if the request is authorized, or otherwise, a signaling rejection message. In the Push scenario, the SP's response includes the signaling message indicating whether or not the request was accepted by the SP.

In addition to the above cases, the attribute defined in this profile may also be used in other contexts; for example, in the Subscription scenario, the SP may include SAML Assertions in its response to vouch for some of SP's identity as the signer of the data objects sent to the SC so that the SC can ensure the authenticity of the data it receives.

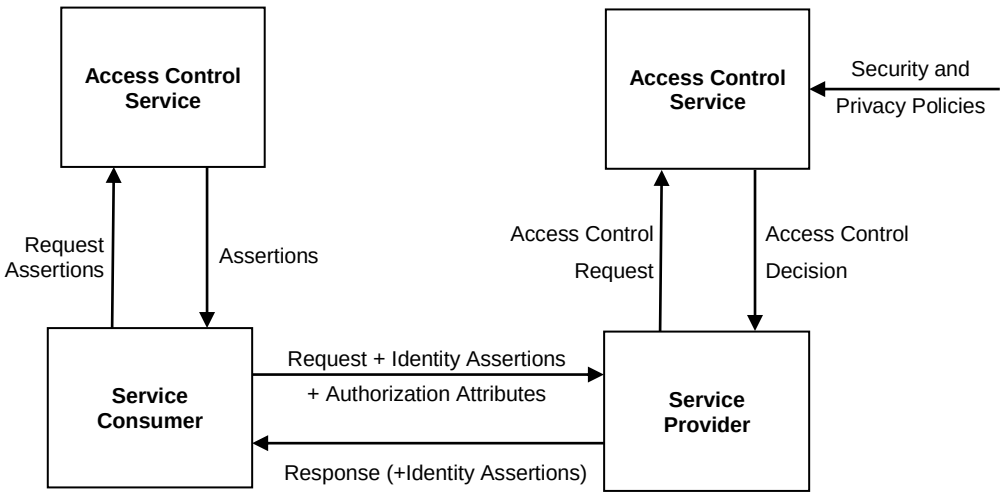

Figure 1: The main event flow in the XSPA use case.

2.1 The Pull Use-Case

The main scenario for Pull is as follows

- The SC initiates a request to access a protected resource residing at the SP.
- If the initiator is a human user, the SC's ACS performs authorization to ensure it is authorized to make such a request. This transaction is outside the scope of this profile.
- The SC sends a request to its ACS, or another trusted Identity Provider, to receive Identity and Authorization Attribute Assertions corresponding to the request, the organization, and the context of the transaction, e.g. purpose of use.
- The SC requests the protected data objects from the SP; the request includes the Identity Assertions and other Authorization Attributes.
- The SP captures the request and calls its own ACS.
- If SP's ACS deems the request authorized, the SP sends a the requested data objects to the SC. This copy is not necessarily identical to the original data; it may be annotated with security labels and handling instructions and/or some portions of it may be redacted or masked depending on the policies.

2.1.1 Variations

The Pull use-case may have some variations.

- **Proactive Pull:** The SC may proactively send a request to SP for a data object (or a group thereof) before a human user specifically requests that data. For example, when an appointment is scheduled for a patient at a facility, the scheduling system at the facility may request the patient's health record in advance, before the physician explicitly asks for it at the time of appointment. This is especially the case when large data volumes need to be exchanged or the connection has a high latency/delay. In such cases, the Principal making the request is a system entity, e.g. the scheduling system, or simply the Service Consumer organization since the SC may not know the identity of the human user which will eventually use the data at the time of data exchange.
- **Delegated Pull:** A Principal may initiate a request on behalf of another Principal, for example, an admin assistant may request a patient's record on behalf of a physician. In such cases, depending on the application, the asserted attributes may include the identity of either of the Principals involved.
- **Poll-Based Subscription:** A Subscription Broker at the SC's side may create a poll-based subscription, meaning that the Broker repeats the request on a regular basis to get a fresh copy of the requested data objects. Depending on the frequency of the poll, the Broker may also re-use the assertions issued by its local ACS if they are still valid or request a fresh set of assertions. This is equivalent to making multiple Pull requests.
- **Notification-Based Subscription:** In a SP-side subscription service, the SC can register with a Subscription Broker at the SP's side to receive a fresh copy of some data objects whenever these data objects are updated. This is equivalent to sending a Pull request and receiving multiple responses.

2.2 The Push Use-Case

The main scenario for Push is as follows:

- The SC initiates a Push request to submit a data object to SP. This may be for creating a new data object or updating an existing one.

- If the initiator is a human user, the SC's ACS performs authorization to make sure the requesting Principal is authorized to make such a request. The current profile does not cover this transaction.
- The SC sends a request to its ACS, or another trusted Identity Provider to receive attribute assertions corresponding to the Principal, the organization, and the transaction.
- The SC sends a Push request to the SP which includes a data object to be submitted to SP as well as the attribute assertions to the request, the organization, and the context of the transaction, e.g. purpose of use.
- The SP captures the request and calls its own ACS.
- If SP's ACS deems the request authorized, the SP consumes the data object and sends back a signaling message to acknowledge the success of the transaction. This may include other information such as the unique identifier assigned to the data object by the server in the case of creating a new data object.

2.3 The Trust Handshake Use-Case

The Trust Handshake is a more general use-case in which the SC approaches the SP with a request to establish trust in order to facilitate future exchange requests. Traditionally, trust handshakes often take place offline and based on manual human negotiations involving technical and legal agreements. As more entities join the exchange market, however, a more dynamic approach is needed in which the SP relies on certifications and attestations by third-parties provided as assertions and in a machine readable form so that it can establish trust with a SC on a dynamic basis.

The flow for this use-case is very similar to the other XSPA flows discussed above, with the difference that it does not specify any specific data objects or any other attributes pertaining to the context of a specific exchange. The attributes provided in this request are only intended to introduce the SC and support the case that the SP can trust the SC for future exchanges. Examples of such attributes are the organization identifier for the SC, its certifications, and policy attestations which denote its compliance with policies or agreements which support the case for a trust relation.

When the SP receives this request, it checks the request attributes against the applicable trust policies. If trust is approved by the applicable policies, the SP accepts the request and notes the SC's identity (e.g. organization identifier) as a trusted partner. Note that the level of trust gained via this protocol can vary and a dynamically trusted SC may be assigned a lower level of trust compared to a partner with manual trust verifications.

Future exchange requests from a trusted SC can proceed more smoothly without repeating the trust handshake.

2.4 Entities

The actors and components existing the XSPA Use-Cases are further discussed in this section.

2.4.1 Service Consumer Access Control Service

The Service Consumer Access Control Service (ACS) provides identity and access control functions to the SC. The Access Control Service resides within the ACS but it may act as a bridge to a third-party Identity Provider (IdP) trusted by the SP.

2.4.2 Service Provider Access Control Service

The Service Provider ACS provides identity and access control functions for the SP. It takes the role of a SAML Relying Party and includes components for parsing assertions. It may also include components for evaluating the assertions against the security and privacy policies and making authorization decisions, Security Labeling Services, and Privacy Preserving Services for enforcing privacy decisions such as masking and redaction. The Service Provider enforces the decisions made by its ACS.

2.4.3 Security and Privacy Policies

Security and privacy policies include the rules that apply to access to protected resources. Such rules are based on various attributes such as the SC identity, purpose of use, security clearance, etc. They may also include obligation rules about labeling the outgoing data objects or privacy modifications such as masking or redaction. This profile does not discuss the details of such policies.

2.4.4 Attributes

Attributes are information pertaining to the access request such as the requesting Principal's identifier, role, organization, and purpose of use which are consequential in making access control decisions.

3 XSPA profile of SAML

The XSPA profile of SAML is an Attribute Profile as defined by Section 2.2 of Profiles for the OASIS Security Assertion Markup Language (SAML) **[SAML-PROF]** which defines the minimum vocabulary necessary to provide access control over resources within and between healthcare systems

This profile is based on the SAML 2.0 core specification. Requests MAY be exchanged using a SAML assertion containing elements such as: `saml2:Issuer` and `saml2:AttributeStatement`.

Although implementations of this profile MAY user `saml2:NameID`, as discussed in Section 3.5, the identity expressed in this element should not be relied on, therefore, the reliable subject identifier must be expressed in the form of an assertion according to SAML v2.0 Subject Identifier Attributes Profile Version 1.0 **[SAML-SUB-ID]**.

3.1 Data Types

Table 1 shows the standard data types used for the attributes defined in this profile. Abbreviated forms will be used in the rest of this document.

Table 1: Standard Data Types (Normative)

Type ID	Abbreviated Form
`http://www.w3.org/2001/XMLSchema#string`	`String`
`http://www.w3.org/2001/XMLSchema#anyURI`	`anyURI`

3.1.1 Concept Descriptor

This profile also defines a special data type, based on Concept Descriptor (CD) data structure **[ISO 21090:2011: 7.5.2 CD]**, commonly used by HL7 **[HL7-Core-Schema-v3]**. The Concept Descriptor data structure captures values defined in the context of a code system.

This profile only supports the Code and Code System elements in the CD data structure. The implementation MAY ignore other elements, such as display names and translations, if present.

This profile defines three different ways to encode Concept Descriptors; the first one is Normative and the latter two are optional if the standard codes used by the implementation can be flattened using the first mechanism.

An implementation MUST use only one of these schemes in a single transaction, i.e. avoid mixing different encodings in a single assertion, although it MAY support more than one of these encodings and choose to use them in different transactions based on parameters beyond the scope of this profile.

3.1.1.1 Flattened Encoding

This profile defines the following scheme to flatten CDs into a value of type `String`:

[Fully-Qualified Unique identifier of the Code System ID]#[Code]

Note that this mechanism presumes that the delimiter, “#”, does not appear in the codes or the code system names, otherwise the implementers MUST use the XML complex datatypes discussed further below in order to avoid any ambiguity.

3.1.1.1.1 Example

{non-normative}

For example, the purpose of “record management” (RECORDMGT) from HL7’s purpose of use vocabulary (2.16.840.1.113883.1.11.20448) can be encoded as the following:

```
<saml:Attribute
       xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name="urn:oasis:names:tc:xacml:2.0:action:purpose"
       xacmlprof:DataType="http://www.w3.org/2001/XMLSchema#anyURI">
  <saml:AttributeValue xsi:type="http://www.w3.org/2001/XMLSchema#anyURI">
       2.16.840.1.113883.1.11.20448#RECORDMGT
  </saml:AttributeValue>
</saml:Attribute>
```

3.1.1.2 Complex Attribute Encoding

{non-normative}

An implementation MAY use complex XML encodings of the Concept Descriptor. This profiles supports the following two complex XML encodings:

- The CD type in HL7 core namespace, urn:hl7-org:v3, or its specializations Coded Equivalent (CE) and Coded Value (CV) **[HL7-Core-Schema-v3]**.
- the code type in HL7 Fast Healthcare Interoperability Resources (FHIR), http://hl7.org/fhir **[HL7-FHIR]**.

3.1.1.2.1 Examples

The following example demonstrate encoding a purpose of use based on the CD type in HL7 core namespace:

```
<saml:Attribute
       xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name="urn:oasis:names:tc:xacml:2.0:action:purpose"
       xacmlprof:DataType="urn:hl7-org:v3:CD">
       <saml:AttributeValue
              xsi:type="urn:hl7-org:v3:CD"
              xmlns:hl7="urn:hl7-org:v3">
             <hl7:value hl7:type="CD"
                    hl7:code="RECORDMGT"
                    hl7:displayName="records management"
                    hl7:codeSystem="2.16.840.1.113883.1.11.20448"
                    hl7:codeSystemName="Purpose of Use" />
       </saml:AttributeValue>
</saml:Attribute>
```

The following example demonstrate encoding a purpose of use based on the code type in HL7 FHIR:

```
<saml:Attribute
       xmlns:xacmlprof="urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML"
       NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
       Name="urn:oasis:names:tc:xacml:2.0:action:purpose"
       xacmlprof:DataType="http://hl7.org/fhir/coding">
       <saml:AttributeValue
              xsi:type=http://hl7.org/fhir/coding
              xmlns:fhir="http://hl7.org/fhir">
            <fhir:code>
              <fhir:system fhir:value="2.16.840.1.113883.1.11.20448" />
              <fhir:code fhir:value="RECORDMGT" />
           </fhir:code>
       </saml:AttributeValue>
</saml:Attribute>
```

3.2 Namespace Requirements

This profile defines the following namespaces:

```
urn:oasis:names:tc:xspa:1.0
urn:oasis:names:tc:xspa:2.0
```

3.3 Attribute Naming Syntax, Restrictions and Acceptable Values

Attribute names MUST adhere to the rules defined by Section 2.7.3.1 of SAML 2.0 Core Specifications **[SAMLCore]**. Additionally, to guarantee interoperability with OASIS eXtensible Access Control Markup Language (XACML), attribute names and values MUST also adhere to the XACML Attribute Profile of SAML **[SAML-PROF:8.5 XACML Attribute Profile]**.

The XML attribute `NameFormat` in `<Attribute>` elements MUST be set to:

```
urn:oasis:names:tc:SAML:2.0:attrname-format:uri
```

The optional XML attribute `FriendlyName` (defined in Section 2.7.3.1 of SAML Core Specifications **[SAMLCore]**) MAY be used to carry an optional string name for human readability.

As prescribed by the XACML Attribute Profile of SAML **[SAML-PROF:8.5 XACML Attribute Profile]**, each attribute element also includes a URI-valued XML attribute called `DataType` in the following XML namespace:

```
urn:oasis:names:tc:SAML:2.0:profiles:attribute:XACML
```

The `DataType` XML attribute MUST be present unless its value can be assumed to be the default, i.e. `String`.

3.4 Attribute Rules of Equality

3.4.1 Attribute Identifiers

Two `<Attribute>` elements refer to the same SAML attribute if and only if their `Name` XML attribute values are equal if and only if they are equal on a Unicode codepoint-by-codepoint basis. The optional XML attribute `FriendlyName` plays no role in the comparison.

3.4.2 Attribute Values

Two attribute values of type `String` or `anyURI` are considered equal if and only if they are equal on a Unicode codepoint-by-codepoint basis.

In complex XML encodings for Concept Descriptor attribute values (as described in Section 3.1.1.2), attribute values are considered equal if and only if their `code` and `codeSystem` values are respectively equal based on the above rule for String equality.

3.5 Subject Identifier

The subject identity, which specifies the identity of the entity which is the subject of the assertions MUST be specified according to SAML v2.0 Subject Identifier Attributes Profile Version 1.0 **[SAML-SUB-ID]**, using either of the following attributes of type `String` defined by that profile.

```
urn:oasis:names:tc:SAML:attribute:subject-id
urn:oasis:names:tc:SAML:attribute:pairwise-id
```

The former is used for universally unique identifiers and the latter is used for identifiers that are only unique between the exchanging partners.

This deprecates the use of the following attribute defined in the previous version of this profile:

```
urn:oasis:names:tc:xspa:1.0:subject:subject-id
```

Note that the subject identifier may correspond to any entity which is the subject of the assertions, including a human user, an organization, or a system entity.

3.6 Attributes

Table 2 shows the list of normative attributes defined by this profile which the implementers MUST support. Table 3 shows the list of deprecated attributes. Future versions of this profile may no longer support these deprecated attributes.

Table 2: Attributes

Required	Identifier[1]	DataType	Description and Valid Values
No	urn:oasis:names:tc:xspa:1.0:subject:organization	String	The name of the requesting organization.
No	urn:oasis:names:tc:xspa:1.0:subject:organization-id	String	The unique identifier of the organization, sub-organization and facility of the Service Consumer. To represent the organizational hierarchy, using urn:oasis:names:tc:xspa:2.0:subject:organizational-hierarchy (below) is preferred.
No	urn:oasis:names:tc:xspa:1.0:subject:child-organization	String	
No	urn:oasis:names:tc:xspa:1.0:subject:facility	String	
No	urn:oasis:names:tc:xspa:2.0:subject:organizational-hierarchy	String	Unique identifiers of the consuming sub-organizations. This is an alternative to using the separate attributes for each level as defined above. Various levels of sub-organizations hierarchy SHOULD be represented as multiple values of type String in order of the most high-level organizational unit to the least.
No	urn:oasis:names:tc:xacml:2.0:subject:role	HL7CD	The requesting Principal's structural role. The values SHOULD belong to a standard vocabulary.
No	urn:oasis:names:tc:xspa:1.0:subject:functional-role	HL7CD	The requesting Principal's functional role. The values SHOULD belong to a standard vocabulary.
No	urn:oasis:names:tc:xspa:1.0:subject:permissions	HL7CD	The requesting Principal's permissions which represent the user's capabilities. The values SHOULD belong to a standard vocabulary.
No	urn:oasis:names:tc:xspa:2.0:subject:confidentiality-clearance	HL7CD	The requesting Principal's confidentiality clearance. The The values SHOULD belong to a standard vocabulary.
No	urn:oasis:names:tc:xspa:2.0:subject:sensitivity-clearance	HL7CD	The requesting Principal's sensitivity clearance. The values SHOULD belong to a standard vocabulary
No	urn:oasis:names:tc:xspa:2.0:subject:integrity-clearance	HL7CD	The requesting Principal's integrity clearances. The values SHOULD belong to a standard vocabulary.

[1] In this and subsequent tables, line-breaks in attribute names are for the purpose of type setting and readability; attribute identifiers are strings with no line-breaks.

Required	Identifier[1]	DataType	Description and Valid Values
No	urn:oasis:names:tc:xspa:2.0:subject:compartment-clearance	HL7CD	The requesting Principal's compartment clearance. The values SHOULD belong to a standard or mutually-agreed vocabulary.
No	urn:oasis:names:tc:xacml:1.0:resource:resource-id	String	Identifier of the data object(s) being requested, e.g. the patient unique identifier, or the query string defining the requested data in case of bulk requests.
No	urn:oasis:names:tc:xspa:2.0:resource:resource-type	HL7CD	The type of data object being requested if applicable. The values SHOULD belong to a standard vocabulary. Deprecates urn:gov:hhs:fha:nhinc:service-type
Yes	urn:oasis:names:tc:xacml:1.0:action:action-id	HL7CD	The identifier of the requested action. The value SHOULD belong to a standard vocabulary.
Yes	urn:oasis:names:tc:xacml:2.0:action:purpose	HL7CD	The purpose of use for the request. The values SHOULD belong to a standard vocabulary.
No	urn:oasis:names:tc:xspa:2.0:subject:supported-obligations	HL7CD	List of obligations that the Service Consumer supports and is able to enforce. The values SHOULD belong to a standard vocabulary.
No	urn:oasis:names:tc:xspa:2.0:subject:supported-refrains	HL7CD	List of refrains that the Service Consumer supports and is able to enforce. The values SHOULD belong to a standard vocabulary such as HL7 Refrains Vocabulary.
No	urn:oasis:names:tc:xspa:2.0:resource:patient-consent-directive	anyURI	The pointer to the patient consent directive corresponding to the requested data objects.
No	urn:oasis:names:tc:xspa:2.0:resource:patient-consent-directive-type	String	The type of patient consent directive. This attribute SHALL NOT be present without a corresponding urn:oasis:names:tc:xspa:2.0:resource:patient-consent-directive attribute.
No	urn:oasis:names:tc:xspa:2.0:subject:certification	String	Certification credentials provided by a jurisdictional or professional body. This attribute is only applicable to the trust handshake use-case.
No	urn:oasis:names:tc:xspa:2.0:subject:policy-attestation	String	Machine-driven assessment of conformance to a known policy or requirement. This attribute is only applicable to the trust handshake use-case.

Table 3: Attributes Planned for Deprecation

Identifier	DataType	Description and Valid Values
urn:oasis:names:tc:xspa:1.0:subject:subject-id	String	Deprecated by Subject Identifier Attributes Profile (see Section 3.5).
urn:gov:hhs:fha:nhinc:service-type	String	Deprecated by: urn:oasis:names:tc:xspa:2.0:resource:type
urn:oasis:names:tc:xspa:1.0:subject:purposeofuse	String	Deprecated by: urn:oasis:names:tc:xacml:2.0:action:purpose

4 Other Considerations

{non-normative}

4.1 Error States

This profile adheres to error states described SAML 2.0 Core Specifications **[SAMLCore].**

4.1 Security Considerations

The following security considerations are established for the XSPA profile of SAML:

- SC and SP have agreed to use this XSPA profile,
- A trust relationship between SP and SC exists ,
- Security and privacy policies have been identified and provisioned,
- The capabilities and location of requested information/document repository services are known,
- Secure channels are established as required by policy,
- Audit services are operational and initialized, and
- Entities have asserted membership in an information domain by successful and unique authentication.

4.1.1 Transmission Security

This profile requires the use of a secure transmission protocol such as HTTPS for exchanging assertions. The implementers MAY choose to encrypt the assertions using the mechanisms defined in SAML.

4.2 Confirmation Identifiers

The manner used by the relying party to confirm that the requester message came from a system entity that is associated with the subject of the assertion will depend upon the context and sensitivity of the data. For confirmations requiring a specific level of assurance, this profile specifies the use of National Institute of Standards and Technology (NIST) Special Publication 800-63 Electronic Authentication Guideline **[NIST-800-63-1]**.

5 JSON Encoding

{non-normative}

Many modern applications use protocols other than SAML which rely on assertions —sometimes referred to as *claims*— which are encoded in JavaScript Object Notation **[JSON]**. This section provides the guidelines for encoding the attributes defined by this profile in protocols relying on JSON. Note that in all JSON snippets in this section, whitespaces are added only for readability and are not a normative part of the data structure.

5.1 Attribute Identifiers

Attribute identifiers defined by this profile can be encoded as JSON strings and implementers MAY choose to use them as such.

When the attribute identifier is used as a key in a JSON object, however, it is often desirable to use simpler identifiers which can be directly mapped to a variable name in a programming language. To enable this and only in cases where the context is unambiguous, the implementers can use simplified attribute identifiers by:

- Dropping the namespace prefix,
- Adding `xspa2_` prefix, and
- Replacing dash ("-") with underscore ("_").

For consistency with standard claims defined by OpenID Connect **[OpenID-Connect: 5.1. Standard Claims]**, the subject identifier attributes MUST be encoded as `sub`. Table 4 shows the simplified JSON encoding of attribute identifiers.

The implementers MUST stick to either of the above JSON encodings for a JSON object and MUST NOT mix the two in a single object.

Table 4: Simplified Attribute Identifiers for JSON Encoding.

Attribute Identifier	Simplified Identifier for JSON Encoding
urn:oasis:names:tc:SAML:attribute:subject-id	sub
urn:oasis:names:tc:SAML:attribute:pairwise-id	sub
urn:oasis:names:tc:xspa:1.0:subject:organization	xspa2_organization
urn:oasis:names:tc:xspa:1.0:subject:organization-id	xspa2_organization_id
urn:oasis:names:tc:xspa:1.0:subject:child-organization	xspa2_child_organization
urn:oasis:names:tc:xspa:1.0:subject:facility	xspa2_facility
urn:oasis:names:tc:xspa:2.0:subject:organizational-hierarchy	xspa2_organizational_hierarchy
urn:oasis:names:tc:xacml:2.0:subject:role	xspa2_role
urn:oasis:names:tc:xspa:1.0:subject:functional-role	xspa2_functional_role
urn:oasis:names:tc:xspa:1.0:subject:permissions	xspa2_permissions

Attribute Identifier	Simplified Identifier for JSON Encoding
urn:oasis:names:tc:xspa:2.0:subject:confidentiality-clearance	xspa2_confidentiality_clearance
urn:oasis:names:tc:xspa:2.0:subject:sensitivity-clearance	xspa2_sensitivity_clearance
urn:oasis:names:tc:xspa:2.0:subject:integrity-clearance	xspa2_integrity_clearance
urn:oasis:names:tc:xspa:2.0:subject:compartment-clearance	xspa2_compartment_clearance
urn:oasis:names:tc:xacml:1.0:resource:resource-id	xspa2_resource_id
urn:oasis:names:tc:xspa:2.0:resource:resource-type	xspa2_resource_type
urn:oasis:names:tc:xacml:1.0:action:action-id	xspa2_action_id
urn:oasis:names:tc:xacml:2.0:action:purpose	xspa2_purpose
urn:oasis:names:tc:xspa:2.0:subject:supported-obligations	xspa2_supported_obligations
urn:oasis:names:tc:xspa:2.0:subject:supported-refrains	xspa2_supported_refrains
urn:oasis:names:tc:xspa:2.0:resource:patient-consent-directive	xspa2_patient_consent_directive
urn:oasis:names:tc:xspa:2.0:resource:patient-consent-directive-type	xspa2_patient_consent_directive_type
urn:oasis:names:tc:xspa:1.0:subject:npi	xspa2_npi
urn:nhin:names:saml:homeCommunityId	xspa2_homeCommunityId
urn:ihe:iti:xca:2010:homeCommunityId	xspa2_homeCommunityId
urn:oasis:names:tc:xspa:2.0:resource:certification	xspa2_certification
urn:oasis:names:tc:xspa:2.0:resource:policy-attestation	xspa2_policy_attestation

5.2 Attribute Values

Attribute values of type `String` and `anyURI` can be encoded straightforwardly in JSON as JSON Strings. When an attribute is multi-valued, the values MUST be encoded using JSON arrays.

For encoding values of type HL7CD, the implementation MUST support the flattened notation described in Section 3.1. Optionally, the implementations MAY also use the following JSON structure:

```
{
  "system": [code system id]
  "code": [code]
}
```

5.2.1 Example

The example attribute assertion from Section 3.1 can be encoded in JSON as either:

```
{
   "xspa2_purpose": "2.16.840.1.113883.1.11.20448#RECORDMGT"
}
```

or:

```
{
   "xspa2_purpose": {
      "system": "2.16.840.1.113883.1.11.20448",
      "code": "RECORDMGT"
   }
}
```

5.3 OpenID Connect Example

The following shows an example of an OpenID Connect claims token in which some of the attributes from this profile are included as additional claims:

```
{
  "sub": "department-1@org1.net",
  "iss": "https://openid.org1.org",
  "aud": "org2",
  "nonce": "hcHlnk,vrjklh",
  "auth_time": 1311280969,
  "iat": 1311280970,
  "exp": 1311281970,
  "xspa2_organization": "Organization One",
  "xspa2_purpose": [
    {
      "system": "2.16.840.1.113883.1.11.20448",
      "code": "RECORDMGT"
    },
    {
      "system": "2.16.840.1.113883.1.11.20448",
      "code": "HOPERAT"
    }
  ]
}
```

6 Conformance

In order to claim conformance, an implementation MUST conform to Section 2 of SAML 2.0 Core Specifications **[SAML]** and comply with the requirements of all subsections of Sections 3 which are not marked as “non-normative,” including the attributes in Table 2.

6.1 US-Realm Conformance

In addition to the above requirements, an implementation in the United States MUST support the US-real attributes in Table 5, and use specific vocabularies for some of the attribute values as described in Table 6. Note that some of these value-sets are extensible and therefore new values can be added to the vocabulary if needed.

Table 5: US-realm Attributes

Required	Identifier	DataType	Description and Valid Values
No	urn:oasis:names:tc:xspa:1.0:subject:npi	String	National Provider Identifier.
No	urn:nhin:names:saml:homeCommunityId and urn:ihe:iti:xca:2010:homeCommunityId	String	The Home Community Identifier as defined by **[NHIN-V3]**. The implementers SHALL interpret these two attributes to be equivalent.

Table 6. Vocabulary Requirements for US-Realm Conformance

Attribute Identifier	Vocabulary
urn:oasis:names:tc:xacml:2.0:subject:role	ASTM Structural Roles Vocabulary **[ASTM E1986-09(2013)]**.
urn:oasis:names:tc:xspa:1.0:subject:permissions	HL7 Healthcare Permissions Vocabulary **[HL7-PERM: Appendix A - Healthcare Permission Tables]**.
urn:oasis:names:tc:xspa:2.0:subject:confidentiality-clearance	HL7 Confidentiality value set (OID: 2.16.840.1.113883.1.11.10228) **[HL7-Vocab]**.
urn:oasis:names:tc:xspa:2.0:subject:sensitivity-clearance	HL7 InformationSensitivityPolicy value set (OID: 2.16.840.1.113883.1.11.20428) **[HL7-Vocab]**
urn:oasis:names:tc:xspa:2.0:subject:integrity-clearance	HL7 SecurityIntegrityObservationValue value set (OID: 2.16.840.1.113883.1.11.20481) **[HL7-Vocab]**.
urn:oasis:names:tc:xspa:2.0:subject:compartment-clearance	HL7 Compartment value set (OID: 2.16.840.1.113883.1.11.20478) **[HL7-Vocab]**.
urn:oasis:names:tc:xspa:2.0:resource:type	HL7 Healthcare Object Codeset **[HL7-PERM: 6.Object Definitions]**.
urn:oasis:names:tc:xacml:1.0:action:action-id	HL7 Healthcare Operations Codeset **[HL7-PERM: 5. Operation Definitions]**.
urn:oasis:names:tc:xacml:2.0:action:purpose	HL7 PurposeOfUse value set (OID: 2.16.840.1.113883.1.11.20448) **[HL7-Vocab]**.
urn:oasis:names:tc:xspa:2.0:subject:supported-obligations	HL7 ObligationPolicy value set (OID: 2.16.840.1.113883.1.11.20445) **[HL7-Vocab]**.

Attribute Identifier	Vocabulary
`urn:oasis:names:tc:xspa:2.0:subject:supported-refrains`	HL7 RefrainPolicy value set (OID: 2.16.840.1.113883.1.11.20446) **[HL7-Vocab]**.

Appendix A. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged:

Participants:

Kel Callahan, HIPAAT International, Inc.

Kathleen Connor, Veterans Health Administration

John M. Davis, Veterans Health Administration

DeCouteau, Duane, Veterans Health Administration

Mohammad Jafari, Veterans Health Administration

Anthony Mallia, Veterans Health Administration

Beth Pumo, Kaiser Permanente

Christopher Shawn, Veterans Health Administration

David Staggs, Veterans Health Administration

Appendix B. Revision History

Revision	Date	Editor	Changes Made
saml-xspa-2.0-wd01	11 Mar. 2012	Duane DeCouteau	Working Draft revisions 01
saml-xspa-2.0-wd02	6 Apr. 2012	Duane DeCouteau	Comments and Changes updated from April 6th TC Meetings.
saml-xspa-2.0-wd03	27 Apr. 2012	Duane DeCouteau	Comments and Changes updated from April 27th TC Meetings
saml-xspa-2.0-wd04	23 May 2012	Duane DeCouteau	Update to organizational-hierarchy purpose of use vocabulary, supported-obligation-policies, supported-refrain-policies
saml-xspa-2.0-wd05	19 Jul. 2013	Mohammad Jafari	Updating the template. Minor editorial corrections.
saml-xspa-2.0-wd05	11 Mar. 2014	Mohammad Jafari	Update to the structure and attribute IDs. - Harmonization with XACML standard attributes.
saml-xspa-2.0-wd05	21 Mar. 2014	Mohammad Jafari	Added HL7 CD data type. Updated the conformance table.
saml-xspa-2.0-wd05	28 Mar. 2014	Mohammad Jafari	Comments from March 25 meeting.
saml-xspa-2.0-csd01	1 Apr. 2014	Mohammad Jafari	Approved by the TC as CSD.
saml-xspa-2.0-wd06	25 Jun. 2014	Mohammad Jafari	Public Review Comments Adding push scenario
saml-xspa-2.0-wd06	10 Sep. 2014	Mohammad Jafari	Resolved OASIS Technical Advisory Board Comments
saml-xspa-2.0-wd06	15 Oct. 2014	Mohammad Jafari	Added US-realm conformance clauses.
saml-xspa-2.0-wd06	25 Nov. 2014	Mohammad Jafari	Added: - Requirement for compliance with XACML Attribute Profile - Requirement for providing DataType XML attributed to guarantee interoperability with XACML. - Correcting CD data type to include URN-based modeling. Allowing alternative XML formats if the ACS implementation can ensure complex data types are supported. - Note on how to fill the NameID of the saml:Subject element.
saml-xspa-2.0-wd07	10 Dec. 2014	Mohammad Jafari	Minor edits
saml-xspa-2.0-wd08	27 Jul. 2015	Mohammad Jafari	Adding new attributes for clearance: Integrity, Compartment, Purpose. Adding a note in the introduction about the consequences of this profile for recording the principal's attributes in audit.
saml-xspa-2.0-wd09	25 Aug. 2015	Mohammad Jafari	Including OIDs for valuesets. Updating clearance attributes. Merging obligations and refrains into caveats. Adding Consent Directive pointer.
saml-xspa-2.0-wd10	16 Mar. 2016	Mohammad Jafari	Editorial corrections.
saml-xspa-2.0-wd11	10 Mar. 2017	Mohammad Jafari	Preparing for the next committee draft.
saml-xspa-2.0-wd12	16 Apr. 2018	Mohammad Jafari	Moving back to working draft to: - Minor edits to the use-case section. - Making some of the attributes non-normative per TC discussions.
saml-xspa-2.0-wd13	24 Sep. 2018	David Staggs	Updated POU to reference HL7 codes, included discussion on medical record access during large scale disasters.
saml-xspa-2.0-wd13	26 Oct. 2018	Mohammad Jafari	Adding short form for attributes when

			encoded in JSON.
saml-xspa-2.0-wd13	2 Nov. 2018	Mohammad Jafari	- SAML subject ID reference and section. Removing reference to NameID. - OpenID reference and conformance for subject IDs. - Clarifying the confusion between normative and required attributes. - Conformance to FHIR flattening style for Concept Descriptors. - Separating examples into non-normative sections.
saml-xspa-2.0-wd14	9 Nov. 2018	Mohammad Jafari	- Finalizing and confirming the HL7 value set references for US realm. Comparing with FHIR and IHE ITI. - Final editorial cleanup.
saml-xspa-2.0-wd15	16 Nov. 2018	Mohammad Jafari	- Equality rule for attribute values. - More clarification around use of HL7 CD. - Add support for CE and CV encodings as specializations of CD on the non-normative section on complex XML encoding. - Add IHE ITI homeCommunityId and its equivalency to the corresponding NHIN attribute.
saml-xspa-2.0-wd16	19 Feb. 2019	Mohammad Jafari	- Adding certification and policy attestation attributes. - Adding the Trust Handshake use-case. - Some Typos. - Updates to participation.
saml-xspa-2.0-wd17	25 Feb. 2019	Mohammad Jafari	- Fixing typos in the examples of Section 5.2.
saml-xspa-2.0-wd18	25 Feb. 2019	Mohammad Jafari	- Fixing typos in the names of the certification and policy attestation attributes.

