

HITSP Access Control Transaction Package

HITSP/TP20



Healthcare Information Technology Standards Panel

Submitted to:

Healthcare Information Technology Standards Panel

Submitted by:

**Security, Privacy and Infrastructure Domain Technical Committee
(Formerly Security and Privacy Technical Committee)**



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Review Copy	Security and Privacy Technical Committee	July 20, 2007
1.0.1	Review Copy	Security and Privacy Technical Committee	October 5, 2007
1.1	Released for Implementation	Security and Privacy Technical Committee	October 15, 2007
	Template Updated to V2.4	Project Team	July 31, 2008
1.1.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	August 20, 2008
1.2	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	August 27, 2008
1.2.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	December 10, 2008
1.3	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	December 18, 2008
	Template V2.5	Project Team	June 30, 2009
1.3.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	June 30, 2009
1.4	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	July 8, 2009
1.4.1	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	November 9, 2009
1.4.2	Review Copy	Security, Privacy and Infrastructure Domain Technical Committee	January 18, 2010
1.5	Released for Implementation	Security, Privacy and Infrastructure Domain Technical Committee	January 25, 2010



TABLE OF CONTENTS

1.0	INTRODUCTION.....	6
1.1	Overview.....	6
1.2	Copyright Permissions.....	6
1.3	Reference Documents.....	6
1.4	Conformance	6
1.4.1	Conformance Criteria	6
1.4.2	Conformance Scoping, Subsetting and Options	6
2.0	TRANSACTION PACKAGE DEFINITION.....	8
2.1	Context Overview	8
2.1.1	Interfaces	9
2.1.2	Interface Interactions	9
2.1.3	Conditions and Assumptions	15
2.2	List of HITSP Constructs	16
2.2.1	Construct Dependencies	16
2.2.2	Additional Constraints on Required Constructs.....	17
2.3	Standards	17
2.3.1	Regulatory Guidance.....	17
2.3.2	Selected Standards	17
2.3.3	Informative Reference Standards.....	18
3.0	APPENDIX	20
3.1	Access Control Implementation.....	20
3.2	Examples of the Application of Access Control.....	21
3.2.1	Process Query to Provide Laboratory Test Result Location(s)	21
3.2.2	Provider Access to Patient Health Information is Verified in Accordance with the Consumer Consent.....	22
3.2.3	Patient Consent Directives (and Security Policies) are Enforced to Allow or Block Access to Patient Health Information	22
3.3	Access Control and Authorization Services	23
3.4	Structural and Functional Roles	23
3.5	Description of Underlying Standards	24
3.5.1	SAML	25
3.5.2	WS-Trust.....	25
3.5.3	XACML	26
3.5.4	WS-Federation	27
3.5.5	Other Standards	27
4.0	CHANGE HISTORY	28
4.1	October 5, 2007	28
4.2	October 15, 2007	28
4.3	July 11, 2008	28
4.4	August 20, 2008	28
4.5	August 27, 2008	28
4.6	December 10, 2008.....	28
4.6.1	Section 1 Updates	28
4.6.2	Section 2 Updates	29
4.7	December 18, 2008	29



4.8	June 30, 2009	29
4.9	July 8, 2009	29
4.10	November 9, 2009	29
4.11	January 18, 2010	30
4.12	January 25, 2010	30

RELEASED FOR IMPLEMENTATION



FIGURES AND TABLES

Figure 2-1 High Level Access Control Interactions.....	9
Figure 2-2 Component Relations in Access Control Interfaces.....	11
Figure 2-3 Detailed Access Control Interface Interaction Diagram.....	12
Figure 3-1 Development of Security and Privacy Protections	20
Figure 3-2 Full List of Permissions from HL7.....	23
Figure 3-3 Role Structure (Adapted from ANSI INCITS Role Model).....	24
Figure 3-4 Access Control Standards	25
Figure 3-5 WS-Trust Security Model.....	26
Figure 3-6 OASIS XACML Components.....	26
Table 1-1 Reference Documents	6
Table 2-1 Interfaces	9
Table 2-2 Context.....	15
Table 2-3 Required Outputs.....	16
Table 2-4 List of Constructs	16
Table 2-5 Construct Dependencies	16
Table 2-6 Additional Constraints on Required Constructs.....	17
Table 2-7 Regulatory Guidance	17
Table 2-8 Selected Standards	17
Table 2-9 Informative Reference Standards	18
Table 3-1 Full List of Permissions from HL7	22



1.0 INTRODUCTION

1.1 OVERVIEW

The Healthcare Information Technology Standards Panel (HITSP) Access Control Transaction Package provides the mechanism for security authorizations which control the enforcement of security policies including: role-based access control, entity based access control, context based access control, and the execution of consent directives. An example of this is a functional role that has the permission to perform an act (e.g., consumer updating a Personal Health Record (PHR)). In an emergency, this construct must support the capability to alter access privileges to the appropriate level (failsafe/emergency access), which may include override of non-emergency consents.

1.2 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

© 2010 ANSI. This material may be copied without permission from ANSI only if and to the extent that the text is not altered in any fashion and ANSI's copyright is clearly noted.

1.3 REFERENCE DOCUMENTS

A list of key reference documents and background material is provided in the table below. HITSP-maintained reference documents can be retrieved from the [HITSP Web Site](#).

Table 1-1 Reference Documents

Reference Document	Document Description
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
TN900 - Security and Privacy	TN900 is a reference document that provides the overall context for use of the HITSP Security and Privacy constructs

1.4 CONFORMANCE

This section describes the conformance criteria, which are objective statements of requirements that can be used to determine if a specific behavior, function, interface, or code set has been implemented correctly.

1.4.1 CONFORMANCE CRITERIA

In order to claim conformance to this construct specification, an implementation must satisfy all the requirements and mandatory statements listed in this specification, the associated HITSP Interoperability Specification, its associated construct specifications, as well as conformance criteria from the selected base and composite standards. A conformant system must also implement all of the required interfaces within the scope, subset or implementation option that is selected from the associated Interoperability Specification.

Claims of conformance may only be made for the overall HITSP Interoperability Specification or Capability with which this construct is associated.

1.4.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

A HITSP Interoperability Specification or Capability must be implemented in its entirety for an implementation to claim conformance to the specification. HITSP may define the permissibility for interface scoping, subsetting or implementation options by which the specification may be implemented in a limited manner. Such scoping, subsetting and options may extend to associated constructs, such as



this construct. This construct must implement all requirements within the selected scope, subset or options as defined in the associated Interoperability Specification or Capability to claim conformance.



2.0 TRANSACTION PACKAGE DEFINITION

2.1 CONTEXT OVERVIEW

The following are the requirements derived from the Harmonization Requests that apply to this construct:

1. Access Control policies are managed (created, modified, deleted, suspended, or restored, and provisioned based on defined rules and attributes)
2. Data access policy is enforced
3. Data access policy exceptions conditions are enforced under positive control (e.g., Emergency access rules ensure that under no conditions are security controls “bypassed”)
4. User data are located by an entity with the ability (privileges) to search across systems
5. Protected data are accessible only through access control decisions based on purpose of use information attributes for subjects, or attributes reflecting resources, actions or the environment
6. Protected data are modified, updated or corrected only by properly authorized users
7. Selected protected data may be blocked from users otherwise authorized to access the information resource
8. Requests for changes to protected data are made by users to providers/sources of data
9. Obligations may be placed upon providing systems prior to granting data access. Obligations may also be placed upon users receiving data that must be honored as a condition or restriction on use

Protected data are defined as any data or information of any type requiring the evaluation and enforcement of access control decisions prior to granting user access.

This construct deals with Access Control. Access Control is principally concerned with the three components of privacy policies, security policies, and enforcing the resulting merged set of policies that are used to determine if access to system resources and functions are to be authorized.

There are four actions that must be completed in order to effectively use this construct:

1. Determining the rules that allow one system to know what to enforce when another system requests access. In the general case, it is assumed that the two systems belong to different domains so that no assumptions can be made about which rules are to be enforced
2. During rule instantiation, collecting and applying the appropriate metadata (Access Control decision information) needed for the rule being enforced at that point in time
3. Making a decision about whether the available Access Control information is sufficient to meet or exceed the access policy requirements for a request
4. Enforcing the decision and any related rules/obligations that must be completed so that the proper request response can be made

This Access Control construct selects the Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) and healthcare profile standards as the baseline authorization attribute exchange protocol that must be supported. In addition, this construct specifies the use of OASIS WS-Trust, which is an extension of WS-Security, as a flexible token-type method for requesting, issuing, renewing, and validating security authorization assertions. The OASIS eXtensible Access Control Markup Language (XACML) and healthcare profile standard are identified as a means to express Security and Privacy policy and obligations in a standards-based, internally consistent way in a number of Harmonization Requests where interoperable policy is required. There is a gap identified where a SAML assertion needs to include a reference to the HTSP/TP30 Manage Consent Directives authorization document location. Health Level Seven (HL7) V3 RBAC, Role Based Access Control Healthcare Permission Catalog (HL7 RBAC) is selected to provide the necessary content for creating interoperable roles. Finally, ASTM International E1986 is selected as a standard terminology for consumers to express preferences that permit machine-enforceable access based on named groups of persons.



HITSP has selected standards which incorporate SOAP. See HITSP/TN907 Common Data Transport - for further discussion on this topic. When the transport is not SOAP, user based access control cannot be enforced on the service side. The client must therefore enforce user level access control where the policy requires it.

2.1.1 INTERFACES

Table 2-1 Interfaces¹

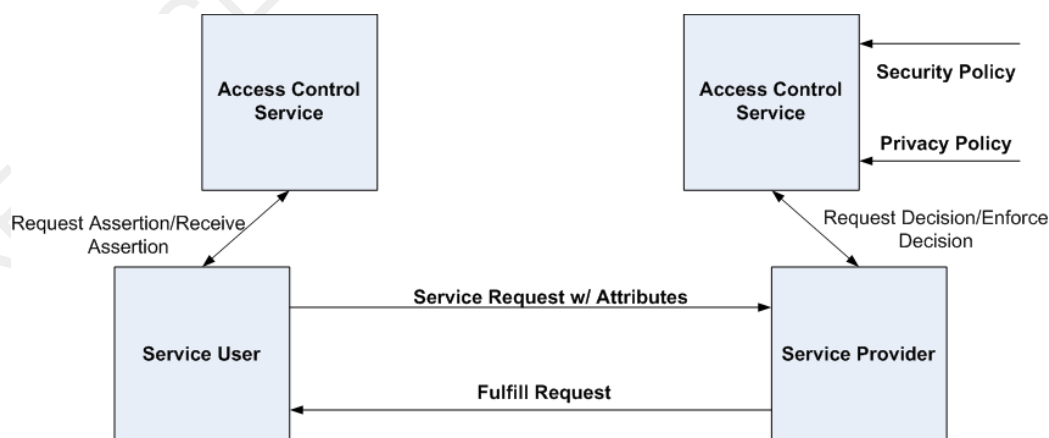
Interface	Description	Used in Component/Composite Standard	Optionality
Access Control Service (ACS)	The Access Control Service is the enterprise security service that supports and implements user-side and/or service side access control capabilities. This service would be utilized by the Service User, and/or Service Provider	WS-Trust, SAML, XACML, HL7 RBAC	R
Service Provider	Represents the system providing a service to all entities that need an assertion or authentication. The service (or assertion) provider is the trusted third party issuer of the trustable identity assertion.	WS-Trust, SAML, XACML, HL7 RBAC	At least one Service User and/or Service Provider is required to be implemented
Service User	The entity represents any individual entity (such as an EHR/PHR system) that needs to make a service request of a Service Provider. The Entity may also be known as a principal and/or entity, which represents an application, a machine, or any other type of entity that may act as a requester in a transaction. A principal is typically represented in a transaction with a digital identity and the principal may have multiple valid digital identities to use with different transactions. Any Service User may also be a Service Provider.	WS-Trust, SAML	At least one Service User and/or Service Provider is required to be implemented

Optionality Legend: "R" for Required, "O" for Optional, or "C" for Conditional

2.1.2 INTERFACE INTERACTIONS

Figure 2-1 provides a high level overview of the typical access control interactions between parties in the exchange of health information. Interfaces described in the figure are explained in Table 2-1 Interfaces above.

Figure 2-1 High Level Access Control Interactions



¹ The Access Control Service Interface is the normative name for the Service User Access Control Service and Service Provider Access Control Service Interfaces.



The interaction between the relevant parties in an access control decision is described as follows:

1. The Access Control Service (ACS) on the Service User side receives the Service User request and responds with a SAML assertion containing user authorizations and attributes
2. To perform its function, the ACS may acquire additional attribute information related to user location, role, purpose of use, and requested resource requirements and actions
3. The ACS on the Service Provider side is responsible for the parsing of assertions, evaluating the assertions against the security and privacy policy, and making and enforcing a decision on behalf of the Service Provider
 - The security policy includes the rules regarding authorizations required to access a protected resource and additional security conditions (location, time of day, cardinality, separation of duty purpose, etc.) that constrain enforcement. Matching the user attributes against the security policy provides the means to determine if access is to be permitted
 - The privacy policy includes the set of organization policies and patient preferences, consent directives, and other privacy conditions (object masking, object filtering, user, role, purpose, etc.) that constrain enforcement. This Transaction Package can retrieve the currently acknowledged consent directives using the Request Consent Directive functionality from HITSP/TP30 Manage Consent Directives
4. The Service User sends the service request with specified attributes. Attributes include access control information (location, role, purpose of use, data sensitivity, etc.) necessary to make an access control decision²

Figure 2-2 provides an expanded view of the Access Control Service modeled after ISO 10181-3 Access Control Framework, exposing this service in the context of its generalized access control information types (per ISO) and associated Service Provider Security and Consent Management activities including two identified interfaces.

Interface 1 includes the service consumer transaction that asserts access control attributes (Access Request Access Control Decision Information (ADI)) intercepted by the Service Provider Access Control Service. Service Consumer ADI along with Resource and any retained Service User (e.g. Subject ADI) and associated contextual Information is provided to the policy decision point to be combined with relevant Security and Privacy rules in order to make an access control decision³. The content of the transactions carrying the Access Request ADI is the subject of Figure 2-3 Detailed Access Control Interface Interaction Diagram⁴

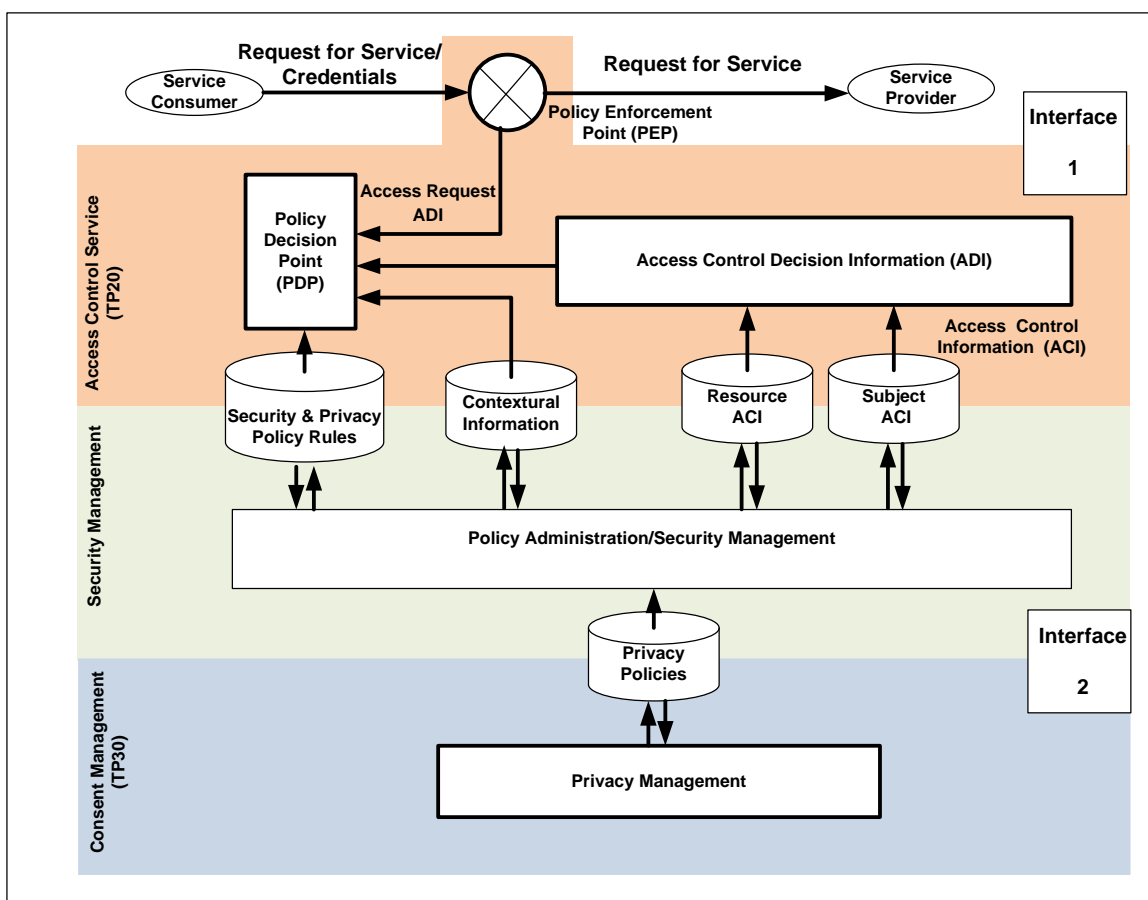
² See ISO 10184-3 for a complete discussion of access control information types.

³ See ISO 10181-3 for a complete discussion of access control information types.

⁴ The details of the generalized Access Control Service functional components are described in ISO 10181-3. The operation of Security Management is outside the scope of this Transaction Package except as a pre-condition.



Figure 2-2 Component Relations in Access Control Interfaces



Interface 2 includes Consent Management as described in HITSP/TP30 Manage Consent Directives. This interface provides the means to convey person privacy policies accepted/agreed to by the Service Provider to Security Management for integration into the Service Provider's composite Security and Privacy Policy Rules. Consent Management also provides the means to consume person privacy policies received from the Service Consumer or from Personal Health Records. Such policies are permitted, but require scrutiny and Privacy Management oversight in order to determine Service Provider acceptance/agreement prior to placing in the directory of Privacy Policies. The Consent Management to Security Management interface is described further in Section 2.1.2.3.1 Enforcing Privacy Consent Directive Policies

The interleaving Security Management layer represents that portion of the Service Provider's internal management processes that links person privacy policy (from Consent Management) with Service Provider (organizational and jurisdictional) policies. Security Management bears overall responsibility for the management of organizational security and privacy policies, provisioning of Resource and Subject ACI and associated Contextual Information, Privilege Management/Identity and Access Management and all other activities surrounding the maintenance and operation of the Service Provider's authoritative secure access control information base.

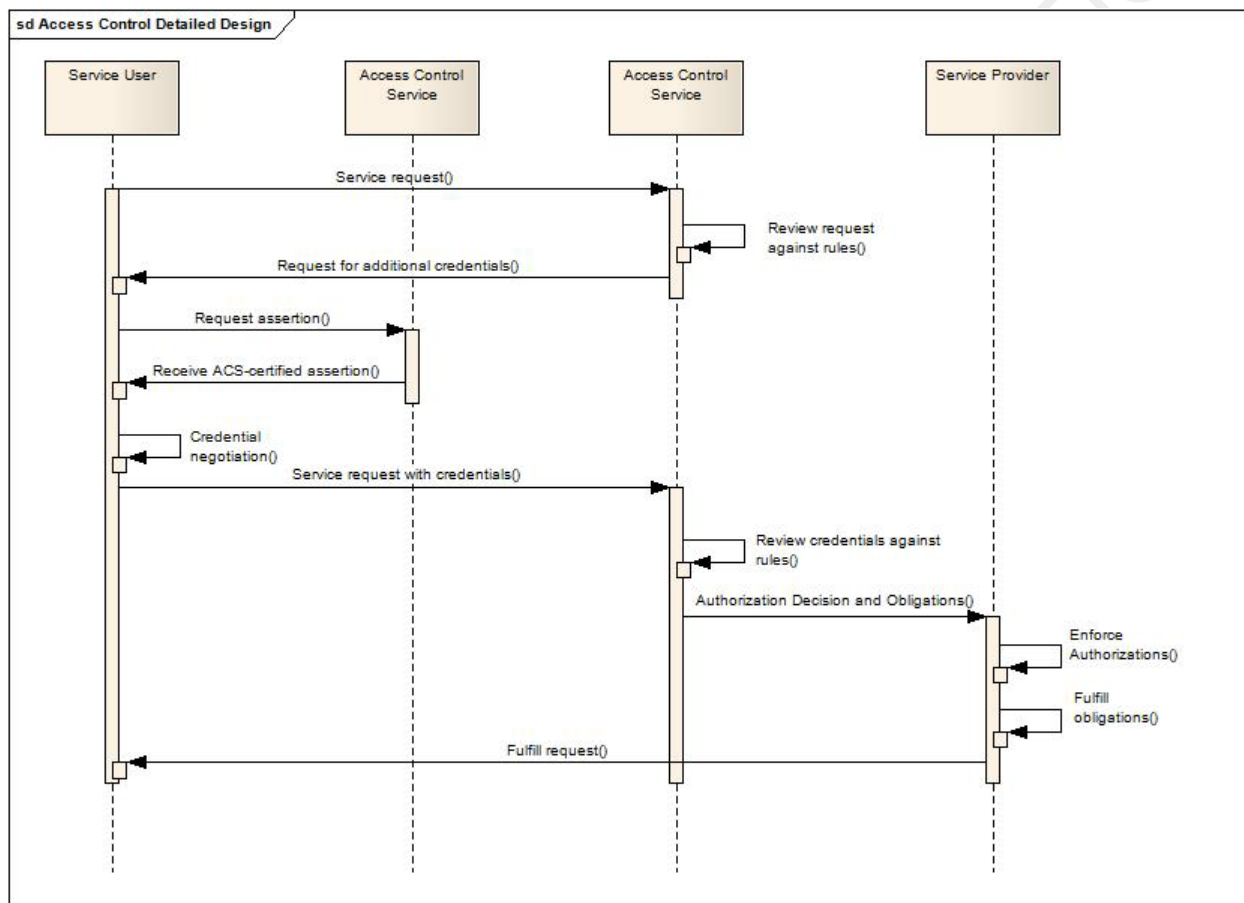
Security Management maps person privacy policy OIDs referenced in the HITSP/TP30 Privacy Policy directories to ACS-executable privacy policy/policy sets. Security Management prepares person originated policies (agreed to by the Service Provider) for linking to existing policy rules and constraints. It is here that Consumer privacy policies are bound to existing organizational and jurisdictional policies to create the complete composite policy/policy sets that will be called upon in the context of a specific



request by a Service Consumer. Security management is a critical function in preparing and provisioning ACI for ACS use, however, Security Management mechanisms are considered proprietary to the internal workings of the Service Provider and their description are therefore out-of-scope of this Transaction Package.

Figure 2-3 provides a more detailed overview of the Access Control interactions that are described as part of this Transaction Package. The Detailed Access Control Interface Interaction Diagram shows the basic process flows for the HITSP Access Control Transaction Package. The standards that frame the interaction are WS-Trust, SAML, XACML, and ATNA (through HITSP/T15 Collect and Communicate Security Audit Trail).

Figure 2-3 Detailed Access Control Interface Interaction Diagram



The pre-conditions needed at the beginning of this construct are specified in Table 2-2 Context.

The interoperability events for the process flows depicted in Figure 2-3 are described as follows:

1. The user initiates the service request (including profiled⁵ token claims)
2. The service request is intercepted by the Service Provider's Access Control Service (ACS). This service examines the request for embedded attributes and assertions, and compares the information provided against the access rules associated with the request

⁵ Profiling refers to a standards-based specification of claim content and allowable value-sets. Claim profiles provide for interoperability.



3. If the service request contains insufficient information for processing (e.g., insufficient authentication or authorization credentials), then the Service Provider ACS will enforce a “fault”
4. On “fault” above, the Service Provider’s ACS responds to the user with a request for additional tokens and provides a description of document side policies that must be met in order to authorize the request (e.g., user must be able to assert permissions of a role, provide patient directives, etc.)
5. The user negotiates and requests needed credentials from the ACS or other source
6. The user responds to the Service Provider’s ACS credential request with a profiled request that includes the needed claims (e.g., tokens)
7. The Service Provider’s ACS verifies the claims and assertions provided against the run time policies for access. As before, if the Service Provider’s ACS finds that the returned credentials are still insufficient to make an initial access control decision, then an “access denied” decision may be enforced, potentially ending the scenario
8. The Service Provider’s ACS forwards the request and authorization decision to the Service Provider. The exact nature of this exchange may vary. The Service Provider’s ACS also communicates any obligations associated with this request to the Service Provider
9. The Service Provider receives the service request, the Service Provider’s ACS decision and any obligations. If additional access decision support is needed, then the Service Provider’s ACS may again be queried. Otherwise, the Service Provider evaluates the request and decisions against any remaining internal rules, constraints, and run time conditions in its own local environment
10. The Service Provider fulfills any obligations (e.g., auditing or information masking) associated with the request and takes appropriate actions (e.g., sends a formatted audit record to the Audit Construct)
11. The Service Provider fulfills the request and provides notification of any cross-enterprise or user side obligations

The post-conditions that need to be in place at the end of this construct are provided in Table 2-6 below.

2.1.2.1 SECURITY ASSERTION MARKUP LANGUAGE (SAML) OVERVIEW

SAML is the baseline authorization attribute exchange protocol that must be supported by use of this technical construct. SAML defines XML-based assertions and protocols, bindings, and profiles. SAML refers to the general syntax and semantics of SAML authorization assertions as well as the protocol (e.g., syntax) used to request and transmit those assertions from one system entity to another. SAML provides authorization statements (e.g., assertions) and a query and response protocol (syntax) for exchanging statements between interfaces. The assertion is a payload in a query and response protocol (e.g., syntax). See HITSP/C19 Entity Identity Assertion for SAML used in the context of authentication ‘identity’ assertions.

SAML supports the following authorization assertion types germane to this construct:

- **Attribute statement:** An attribute statement asserts that a subject is associated with certain attributes used to make access control decisions for a particular security policy

2.1.2.1.1 SAML Healthcare Profile

For defining the mandatory and optional value sets required for interoperability, this Transaction Package specifies the OASIS Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare Version 1.0," November 2009 (U.S. realm). The XSPA profile of SAML provides access control information needed to make access control decisions for controlling security and functionality within and between health information technology (IT) systems.

2.1.2.2 WS-TRUST OVERVIEW

This Transaction Package specifies the use of WS-Trust, an extension of WS-Security, as a token type agnostic method for requesting, issuing, renewing, and validating security authorization assertions.



Entities needing to exchange complex access control information attributes, as described below, may use the OASIS WS-Trust standard in lieu of SAML or in conjunction with it, based upon a pre-negotiated agreement. The core component of WS-Trust is the Security Token Service (STS). WS-Trust involves interactions between a service requestor, STS and service provider. WS-Trust provides statements called claims and a request RQST/response and RQSTR/protocol. The ACS includes the STS as an embedded capability.

WS-Trust applies to access control information exchanges where the need to describe complex security policy exceeds what can be provided by SAML Attribute Assertions and Decisions.

2.1.2.2.1 WS-Trust Healthcare Profile

If WS-Trust is used, then this Transaction Package specifies the use of the OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) WS-Trust Healthcare (U.S. Realm) Profile. The XSPA profile of WS-Trust provides cross-enterprise authorization of entities within and between health IT systems by providing common semantics and vocabularies for interoperable course and fine grained access control. This standard is provided only as an informative reference at this time.

2.1.2.3 XACML OVERVIEW

XACML together with the WS-Trust Security Token Service define core capabilities of this construct's Access Control Service. XACML is a general purpose language for specifying access control policies. In XML terms, it defines a core schema with a namespace that can be used to express access control and authorization policies for XML objects. XACML provides features that make it possible to support a broad range of policies. It provides the capability to request a specified action within a system using a standardized syntax, and then receive one of four replies:

- Permit – action allowed
- Deny – action disallowed
- Indeterminate – error or incorrect/missing value prevents a decision
- Not Applicable – request cannot be processed

This construct specifies the use of OASIS XACML as a means to express Security and Privacy policy and obligations in a standards based, internally consistent way.

2.1.2.3.1 Enforcing Privacy Consent Directive Policies

This Access Control construct is expected to enforce consent directives from HITSP/TP30 Manage Consent Directives. At this time HITSP/TP30 Manage Consent Directives are simple acknowledgements by the consumer to one or more policies as stated by Object Identifiers (OID). Therefore, the Access Control decision can gain access to the currently acknowledged consent directives through the use of the Request Consent Directive transaction from HITSP/TP30 Manage Consent Directives, where necessary. When the consent directive is managed in a HITSP/TP13 Manage Sharing of Documents environment, the request for consent directives is a simple web-service request using a patient identifier, and asking for the list of currently acknowledged consent directives. The returned output is zero or more OIDs that are currently acknowledged. The Access Control engine is expected to know the rules associated with each of the OIDs.

As described in HITSP/TP30 Manage Consent Directives, HL7 Version 3 encoded or BPPC unencoded privacy policies, records of consumer acknowledgement, assent or dissent, and consumer specific consent directives may be referenced by confidentiality codes associated with protected health information. Metadata about protected health information that include associated confidentiality codes will specify the address of the repository in which the referenced privacy policy, record of consumer acknowledgement, assent/dissent, or consent directive is persisted. Enterprise services request the artifacts referenced by confidentiality codes using HITSP/TP13 Manage Sharing of Documents



mechanisms in order to provision policy information points within the ACS when there is no locally persisted data.

2.1.2.3.2 XACML Healthcare Profile

XACML is used to describe the interaction between the ACS Policy Enforcement Point (PEP) and Policy Decision Point (PDP). As HITSP/TP20 Access Control describes only the required transaction between participating ACS, the details of the internal ACS implementation is out of scope. If XACML is used, then this Transaction Package identifies the Organization for the Advancement of Structured Information Standards (OASIS) Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0," November 2009. The XSPA Profile of XACML provides common semantics and vocabularies for interoperable cross-enterprise security and privacy policy exchange among entities within and between health IT systems interoperable with the XSPA SAML Profile.

2.1.3 CONDITIONS AND ASSUMPTIONS

Table 2-2 Context

Assumptions, Pre-conditions, Post-conditions, and Triggers	Type of Context
It is expected that the security framework under which this Transaction Package operates is in accordance with the HITSP Interoperability Specification that references this construct. Therefore, all applicable HITSP Security and Privacy constructs are implemented as required	Pre-condition
Entities must have been identified and provisioned (credentials issued, privileges granted, etc.)	Pre-condition
Privacy policies are identified and provisioned (consent directives, user preferences, etc.) in appropriate components in accordance with policy	Pre-condition
Appropriate cross-domain security policies are defined	Pre-condition
Policies are written and available to a PDP in a vocabulary it can understand and process. This is not currently achieved with a HITSP construct. But under local administration, within a domain, they can assign their own vocabulary to use	Pre-condition
Pre-existing Security and Privacy policies are provisioned to access control services	Pre-condition
Pre-existing trust relationships necessary between Access Control Services have been established	Pre-condition
Agreements regarding protocols, (SAML, WS-Trust) tokens, token types, and keys are negotiated in advance	Pre-condition
The capabilities and location of requested information/document repository services are known	Pre-condition
Secured channels are established as required by policy in accordance with HITSP/T17 - Secured Communication Channel	Pre-condition
Audit services are initialized in accordance with HITSP/T15 - Collect and Communicate Security Audit Trail	Pre-condition
Entities have asserted membership in an information domain by successful and unique authentication consistent with the HITSP/C19 - Entity Identity Assertion. Each entity must have credentials and the ability to authenticate separately from any other entity	Pre-condition
Requests for updates/append to data by patients have been received and approved	Pre-condition
Support for enterprise wide distributed authorization (e.g., identified enterprise Security and Privacy policies, cross-domain business oriented least privilege, separation of duty and need-to-know policies, business partner access agreements and policies, patient consents, and user profiles) is in place and supported by ACS and Authorization Mechanisms	Pre-condition
RBAC and role engineering, with identified structural and functional roles, is supported by ACS and Authorization Management in accordance with this constructs profiles	Pre-condition
An emergency access context, with associated policies and authorizations, is supported by ACS and Authorization Management	Pre-condition
Consumer preference requests have been received, reviewed and approved for organizational enforcement in accordance with applicable policy and law	Pre-condition
Privacy policies are provisioned (organization agreed-to consumer consent directives/preferences, as well as organizational/jurisdictional privacy policies, etc.) in appropriate ACS components per established rules and agreements	Pre-condition



Assumptions, Pre-conditions, Post-conditions, and Triggers	Type of Context
Security policies are provisioned (organizational/jurisdictional security policies, cross-domain security policies, etc.) in appropriate ACS components per established rules and agreements	Pre-condition
Security and privacy access control information (including contextual information) are known and provisioned to ACS components	Pre-condition
Mechanisms for making resource metadata known, including access policies have been established and metadata provisioned	Pre-condition
Request for protected resources (e.g., protected information, protected functionality, etc.)	Trigger
Access is authorized or denied. If access is permitted, then the PEP permits access to the resource; otherwise, it denies access	Post-condition
Issued credentials that are no longer required are cleaned up	Post-condition
Any requirements and obligations on enterprise systems are fulfilled (e.g., audit events are recorded)	Post-condition
Entities must be members of defined information domains under the authorization control of a defined set of policies	Constraint
The Transaction Package applies to any circumstance in which authorizations need to be adjudicated for access to protected information	Constraint

2.1.3.1 REQUIRED OUTPUTS

Table 2-3 Required Outputs

Required Output	Format/Usage
Audit events are recorded and alerts communicated	Specified in HITSP/T15 – Collect and Communicate Security Audit Trail
Request is fulfilled. (The service fulfills the request and returns the resource information to the client)	HL7 v3.0 CDA
Obligations on users and user Enterprise ACS are forwarded	XACML Obligation wrapped in OASIS SAML V2.0 protocol over OASIS SOAP V1.0 using HL7 Confidentiality codes or “Constraints”

2.2 LIST OF HITSP CONSTRUCTS

Table 2-4 List of Constructs

Construct Name	Description
HITSP/T15 – Collect and Communicate Security Audit Trail	The HITSP Collect and Communicate Security Audit Trail Transaction is a means to provide assurance that security policies are being followed or enforced and that risks are being mitigated. This document describes the mechanisms to define and identify security relevant events and the data to be collected and communicated as determined by policy, regulation or risk analysis. It also provides the mechanism to determine the record format to support analytical reports that are needed
HITSP/TP30 – Manage Consent Directives	The HITSP Manage Consent Directives Transaction Package describes the messages needed to capture, manage, and communicate rights granted or withheld by a consumer to one or more identified entities in a defined role to access, collect, use or disclose Individually Identifiable Health Information (IIHI), and also supports the delegation of the patient's right to consent. The transactions described in this construct are intended to be carried out by HITSP/TP13 Manage Sharing of Documents

2.2.1 CONSTRUCT DEPENDENCIES

Table 2-5 Construct Dependencies

Construct	Depends On (Name of construct that it depends on)	Dependency Type (Pre-condition, Post-condition, General)	Purpose (Reason for this dependency)
HITSP/TP20 – Access Control	HITSP/C19 – Entity Identity Assertion	General	Users of the system are identified



2.2.2 ADDITIONAL CONSTRAINTS ON REQUIRED CONSTRUCTS

Table 2-6 Additional Constraints on Required Constructs

Constraint ID	Data Element	Construct	Constraint	Constraint Type (Pre-condition, Post-condition, general)	Purpose (Reason for this constraint)
No applicable constraints					

2.3 STANDARDS

2.3.1 REGULATORY GUIDANCE

Table 2-7 Regulatory Guidance

Regulation	Description
No applicable regulatory standards	

2.3.2 SELECTED STANDARDS

Table 2-8 Selected Standards

Standard	Description
Health Level Seven (HL7) V3 RBAC, R2-2009, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 2, October 2009 ⁶	The Healthcare Permission Catalog provides the necessary content for creating interoperable roles facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit www.hl7.org
Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) Core v2.0 OASIS Standard; ITU-T X.1141	SAML, developed by the Security Services Technical Committee of OASIS, is an XML-based framework for communicating user authentication, entitlement, and attribute information. As its name suggests, SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (an entity that is often a human user) to other entities, such as a partner company or another enterprise application. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare Version 1.0," November 2009	The XSPA SAML profile provides the necessary content for exchange interoperable access control information facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) WS-Trust Version 1.3, March 2007	Defines extensions that build on [WS-Security] to provide a framework for requesting and issuing security tokens, and to broker trust relationships. Defines Security Token Service (STS) model for security tokens including requesting, issuing, renewing, canceling and validating. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML), ITU-T Recommendation X.1142, February 2005	The Organization for the Advancement of Structured Information Standards (OASIS) standards group developed the eXtensible Access Control Markup Language (XACML) as a language to express and evaluate access decisions. The XACML technical specification includes a profile for RBAC using XACML that complies with the ANSI RBAC standard. The HL7 RBAC Permission Catalog provides a standard vocabulary that can be used for cross-enterprise access control. For more information visit www.oasis-open.org
ASTM International #E1986 -98 (2009) Standard Guide for Information Access Privileges to Health Information	The guide covers the process of granting and maintaining access privileges to health information. In particular, Table 2 Healthcare Personnel that Warrant Differing Levels of Access Control provides the necessary content for structural roles per ASTM International E2595 and for user-based access controls enforcing patient consent directives

⁶ Note this standard is to be updated following ANSI acceptance.



2.3.3 INFORMATIVE REFERENCE STANDARDS

Table 2-9 Informative Reference Standards

Note: The following table lists standards that provide additional background information or guidance; however, they are not required for the implementation of this Transaction Package specification. In addition, it should be noted that HITSP is entertaining discussion of other Access Control policy languages that may be appropriate for different platforms, and subsequently may be added to this list of informative reference standards.

Standard Name	Reason for Use
American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS), #359-2004	This standard describes RBAC features that have achieved acceptance in the commercial marketplace. It includes a reference model and functional specifications for the RBAC features defined in the reference model. It is intended for (1) software engineers and product development managers who design products incorporating access control features; and (2) managers and procurement officials who seek to acquire computer security products with features that provide access control capabilities in accordance with commonly known and understood terminology and functional. For more information visit www.ansi.org
ASTM International Standard Guide for Privilege Management Infrastructure (PMI) Guidelines: #E2595-07	Defines interoperable mechanisms to manage privileges in a distributed environment. This standard is oriented towards support of a distributed or service-oriented architecture (SOA) where security services are themselves distributed and applications are consumers of distributed services. This standard incorporates privilege management mechanisms alluded to in a number of existing standards (e.g., E1986, E2084). The privilege mechanisms in this standard support policy-based access control (including role, entity and contextual-based access control) including the application of policy constraints, patient requested restrictions and delegation. Finally, the standard supports hierarchical, enterprise-wide privilege management. The mechanisms defined in this standard may be used to support a privilege management infrastructure (PMI) using existing public key infrastructure (PKI) technology. This standard does not specifically support mechanisms based on secret-key cryptography. Mechanisms involving privilege credentials are specified in International Organization for Standardization (ISO) 9594-8:2000 (attribute certificates), and Organization for the Advancement of Structured Information Standards (OASIS) Security Assertion Markup Language (SAML) (attribute assertions); however, this standard does not mandate or assume the use of such standards. Many current systems require only local privilege management functionality (on a single computer system). Such systems frequently use proprietary mechanisms. This standard does not address this type of functionality; rather, it addresses an environment where privileges and capabilities (authorizations) must be managed between computer systems across the enterprise, and with business partners. For more information visit www.astm.org
Health Level Seven (HL7) Consent related vocabulary including Confidentiality Codes	HL7 concept domains, including ConfidentialityCodes, ActInformationCategoryCode, ActInformationAccessType, ActInformationAccessContextCode, AuthorizedParticipationFunctionCode, ActPolicyType, ActConsentType, and ActMaskableCode For more information visit www.hl7.org
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0 or later, Audit Trail and Node Authentication Profile (ATNA)	Audit Trail and Node Authentication (ATNA) establishes the characteristics of a Basic Secure Node. It describes the security environment (user identification, authentication, authorization, access control, etc.) assumed for the node so that security reviewers may decide whether this matches their environments. It defines basic auditing requirements for the node. It defines basic security requirements for the communications of the node using TLS or equivalent functionality. It establishes the characteristics of the communication of audit messages between the Basic Secure Nodes and Audit Repository nodes that collect audit information. This integration profile has been designed so that specific domain frameworks may extend it through an option defined in the domain specific technical framework. Extensions are used to define additional audit event reporting requirements, especially interface specific requirements. For more information visit www.ihe.net



Standard Name	Reason for Use
International Organization for Standardization (ISO) Health Informatics -- Information technology -- Text and office systems - Office Document Architecture (ODA) and interchange format, Technical Report on ISO 8613 Implementation Testing, Technical Specification # ISO/IEC CD 10183 -- Part 3: Testing procedure	Specifies a general framework for the provision of access control. The purpose of access control is to counter the threat of unauthorized operations involving a computer or communication system. For more information visit www.iso.org
International Organization for Standardization (ISO) Health Informatics -- Privilege management and access control (PMAC), Technical Specification #22600 -- Part 1: Overview and policy management, July 2006	Supports the needs of healthcare information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, their patients, staff members and trading partners. It is also intended to support inquiries from both individuals and application systems. For more information visit www.iso.org
In International Organization for Standardization (ISO) Health Informatics – Functional and Structural Roles (ISO SF Roles), Technical Specification #21298 , Draft May, 2007	This document contains a specification for encoding information related to roles for health professionals and consumers. At least four areas have been identified where a model for encoding role information is needed. 1. Privilege management and access control: role-based access control is not possible without an effective means of recording role information for healthcare interfaces. 2. Directory services: structural roles are usefully recorded within directories of healthcare providers (see for example, ISO TS 21091 Health Informatics – Directory services for security, communications, and identification of professionals and patients). 3. Audit trails: functional roles are usefully recorded within audit trails for health information applications. 4. Public key infrastructure (PKI): The three part ISO standard 17090 Health Informatics – Public Key Infrastructure (PKI) allows for the encoding of healthcare roles in certificate extensions, but no structured vocabulary for such roles is specified. This technical specification identifies such a coded vocabulary. For more information visit http://www.iso.org/www.iso.org
Organization for the Advancement of Structured Information Standards (OASIS) Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0," November 2009	The XSPA XACML profile provides the necessary content for evaluating principal access control information against established security policy and making access control decisions enforcing established security policy. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) WS-Federation Web Services Federation Language (WS-Federation), Version 1.2 Committee Draft 01 June 23, 2008	Defines mechanisms to allow different security realms to federate, such that authorized access to resources managed in one realm can be provided to security principals whose identities and attributes are managed in other realms. This includes mechanisms for brokering of identity, attribute, authentication and authorization assertions between realms, and privacy of federated claims. For more information visit www.oasis-open.org
Organization for the Advancement of Structured Information Standards (OASIS) Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of WS-Trust for Healthcare, Committee Draft, 14 October 2008	The XSPA WS-Trust profile provides the necessary content for exchange interoperable access control information facilitating inter-organizational communications and information sharing among healthcare organizations and their business partners
International Health Terminology Standards Development Organisation (IHTSDO) Systematized Nomenclature of Medicine Clinical Terms (SNOMED CT®)	SNOMED CT consists of a technical design, core content architecture, and Core content. SNOMED CT Core content includes the technical specification of SNOMED CT and fully integrated multi-specialty clinical content. The Core content also includes a concepts table, description table, relationships table, history table, ICD-9-CM mapping, and Technical Reference Guide. Additionally, SNOMED CT provides a framework to manage language dialects, clinically relevant subsets, qualifiers and extensions, as well as concepts and terms unique to particular organizations or localities. For more information visit www.ihtsdo.com



3.0 APPENDIX

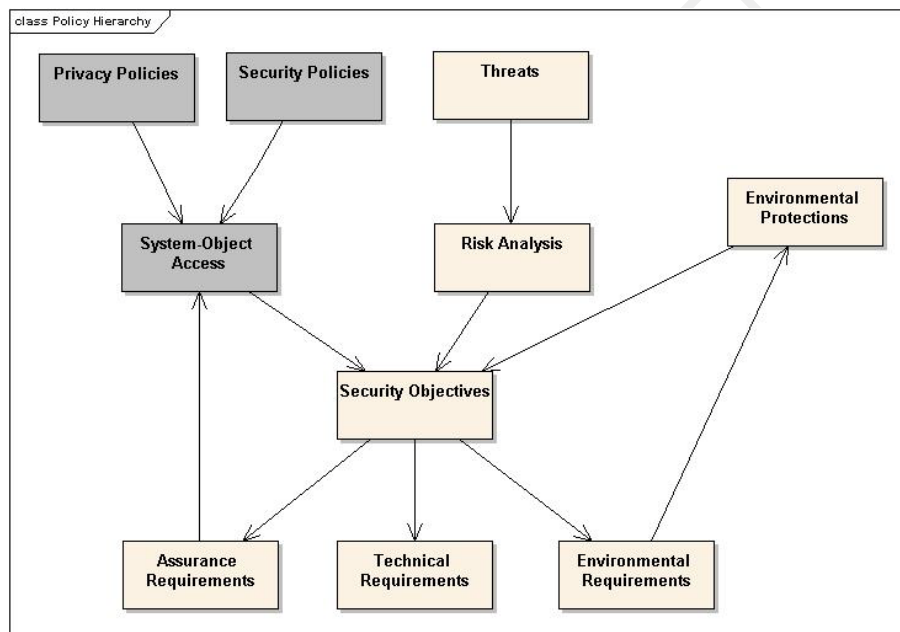
The following sections include relevant materials referenced throughout this document.

3.1 ACCESS CONTROL IMPLEMENTATION

The ISO-10183 (ISO AC) standard specifies a general framework for the provision of Access Control. The ISO PMAC standard supports the needs of health information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, patients, staff members, and trading partners. ISO Structural and Functional Roles provide guidance for creating roles, by defining and describing some roles based upon European business models.

The following diagram illustrates a way to view the development of Security and Privacy protections. The shaded boxes are the portions of this model that apply to this Transaction Package. Further discussion on policy can be found in HITSP/TN900 Security and Privacy Technical Note.

Figure 3-1 Development of Security and Privacy Protections



Privacy policies are statements of desired protections to be provided to subjects of the data, e.g., patients.

Security policies are statements of desired protections to be provided to the information technology (IT) system functions and data. This includes protection of the underlying security functions themselves. ISO 22600-1 and 2 provide the framework and models for security management used in this construct.

System-object access policies are the merged set of Security and Privacy policies, focusing on access controls. In some cases there are conceptual duplications and synergies identified and handled by this merger.

Assurance requirements are the set of activities during system design, implementation, and operation to assure that system-object access policies are being fulfilled and risks are being mitigated. These can include activities like component selection, documentation, training, reading audit log reports, periodic penetration tests, etc.



Privacy policy includes policies that may be defined by regulatory bodies, are established and followed by healthcare organizations, and that consumers wish the system to implement as specified in their consent directives. Privacy policy management involves granting privacy attributes to clinicians and systems and managing and instantiating privacy policy within the application security mechanisms. Privacy policies, as they relate to Access Control, define restrictions or limitations around four main aspects of Access Control:

1. Who can access the data
2. What data can be accessed by those being granted access
3. When can the data be accessed
4. For what purpose is the data being allowed to be accessed

Security policy management includes the policies that the enterprise wishes the system to enforce such as requirements of law, regulation or business rule. Constraints modify these rules and obligations imposing actions on system components that must be honored prior to granting access. Security policy management includes granting security attributes to users and provisioning these to the various components of the security system.

Security policy enforcement (Access Control) deals with ensuring that users attempting to access system functions and data possess attributes (such as privileges granted and provisioned in Security and Privacy management) equal to or greater than that required for the access. Access Control considers other relevant information needed to make and then enforce an Access Control decision. ISO 10181-3 provides the framework and models for Access Control. This standard also defines the different types of access control information used in this Transaction Package.

3.2 EXAMPLES OF THE APPLICATION OF ACCESS CONTROL

The following examples are provided to illustrate how Access Control is applied firstly in a scenario where there is a query for laboratory test results, a second scenario in which there is a need to verify consumer consent for provider access to patient health information, and lastly a scenario in which patient consent directives (and security policies) are enforced to allow or block access to patient health information.

3.2.1 PROCESS QUERY TO PROVIDE LABORATORY TEST RESULT LOCATION(S)

This section provides an example of the EHR-Lab Event 3.5.2.0 from the Harmonization Request for Electronic Health Records (Laboratory Results Reporting) (EHR-Lab), applied to the Access Control models described in the sections above.

The following pre-conditions are directly extracted from the EHR-Laboratory Results Reporting Harmonization Request:

1. Users of the system are identified
2. Identified users of the system are provided with their login credentials (tokens)
3. Identified users are assigned to their appropriate group
4. Identified users update their login information
5. Users and groups are managed in an enterprise and across enterprises
6. Directory services are managed in an enterprise and across enterprises
7. User data are located by an entity with the ability to search across systems
8. Registration data are modified, updated or corrected by identified users

Item 1 is satisfied using the HITSP/C19 Entity Identity Assertion. Items 2 - 8 are necessary requirement elements for managing user credentials that are not yet addressed by a HITSP construct.

In addition to the above pre-conditions that are imposed by the scenario example, the pre-conditions described in Table 2-2 are also expected. Specifically, Policy Administration Points (PAP) writes policies and policy sets and makes them available to the Policy Decision Point (PDP). These policies or policy sets represent the complete policy for a specified target and include security and privacy policies. The



HITSP/TP30 Manage Consent Directives describes how to create/assemble a set of privacy policies (consent directives and authorizations). The Access Control construct deals with instantiated policies that HITSP/TP30 expresses. HITSP/TP30 is the engine that creates an authoritative set of policies to put in place, and then this Access Control construct enforces those policies.

3.2.2 PROVIDER ACCESS TO PATIENT HEALTH INFORMATION IS VERIFIED IN ACCORDANCE WITH THE CONSUMER CONSENT

This example illustrates the relationship between HITSP/TP30 Manage Consent Directives and this construct. The Access Control decision may need to include verification of consumer consent acknowledgement (see HITSP/TP30) to ensure that the consumer has allowed for and continues to support the use of the data. The Access Control decision will need to enforce the appropriate use as defined by the confidentiality code attributes that define the privacy policy (or policies) to be evaluated. Specific required attributes for subjects, resources, actions, and environment necessary to evaluate the policy are included in the policy set. The context handler retrieves the current values for these attributes, which may include identification of the patient, clinician, environment (e.g., time of day) and optionally resource content (steps 6-9 described in the Interoperability events section above). The context handler provides these values to the Policy Decision Point (step 10 of Interoperability events described above).

It is also necessary to verify provider access to patient health information in accordance with applicable security policy. These policies may include business rules for access as well as constraints such as separation of duty, cardinality (e.g., the number of individuals who may be concurrently asserting a specific role such as head nurse), time of day, or other environmental factors. In determining role-based Access Control, evaluation of the policy rules allow for a decision based upon user's roles or permissions provided in the applicable claimant token. These are specified by reference to subject attributes of the HL7 Permission Catalog, which in this example includes review permissions of Laboratory Orders.

Table 3-1 Full List of Permissions from HL7

Scenario ID	Unique Permission ID	Abstract Permission Name	Basic Permission Name {Operation (R=Read), Object}
SRD-001	PRD-004	Review Existing Order(s)	{R, Laboratory Order}

The specifics of the System-object Access policy are determined using the HITSP/TP30 Manage Consent Directives construct for Policy Information Point (PIP) supplied attribute values of subject, resource, actions, and environment. These attribute values are specified in the policy, or optionally, in the resource content. The policy attributes may point to HITSP/TP30 Manage Consent Directives and be retrieved from the Consent Directive Repository. The policies themselves are pre-conditions as currently described. Interoperability requirements will require the definition of appropriate vocabularies (this is identified as a gap in HITSP/TN900 Security and Privacy).

Verification also means the evaluation of the request policy based upon the policy set and applied attributes germane to both security and privacy. The Policy Decision Point informs the Policy Enforcement Point of the decision via the response context.

3.2.3 PATIENT CONSENT DIRECTIVES (AND SECURITY POLICIES) ARE ENFORCED TO ALLOW OR BLOCK ACCESS TO PATIENT HEALTH INFORMATION

The enforcement of both patient consent directions and access to medication data are based upon a single composite decision of the Policy Decision Point which has evaluated a combined security and privacy policy set and applied attributes.

Prior to allowing access, the Policy Enforcement Point must be able to fulfill any outstanding obligations. In the case of an Access Control decision, this may include audit (using HITSP/T15 Collect and Communicate Audit Trail), masking directives (if not already specified by resource policy as a required output), or further obligations to be passed to an external Access Control system for enforcement of consumer directives.

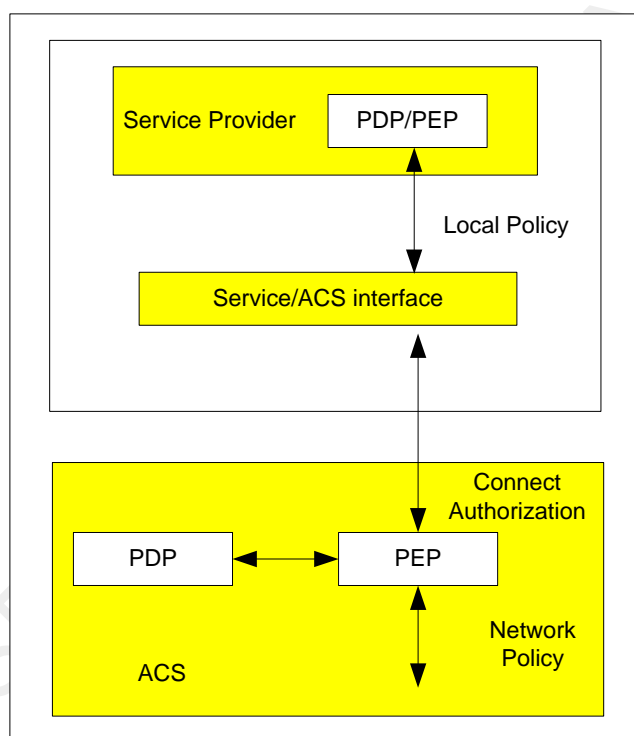


The post-conditions are specified in Table 2-2. Specifically for this example, registration and medication data are accessed based on user permission (and privacy policies) for data access. Selective registration data or medication data are blocked from users, and requests for changes to registration or medication data are made by users to providers/sources of data. The required outputs are shown in Table 2-3.

3.3 ACCESS CONTROL AND AUTHORIZATION SERVICES

Figure 3-2 illustrates an access decision and enforcement environment for a healthcare information system. In the model, high-level “role-groups” (slow-changing enterprise roles)⁷ are used by the distributed authentication and authorization infrastructure belonging to the ACS to provide “connect” access to the protected end system resources. Once connected, it will be necessary to evaluate and verify the application-level permissions (functional roles) owned by the user, other security policy, and the privacy policy in order to access the application data and functions. As illustrated, network and end system Policy Decision Point and Policy Enforcement Point collaborate to make Access Control decisions.

Figure 3-2 Full List of Permissions from HL7



3.4 STRUCTURAL AND FUNCTIONAL ROLES

This construct distinguishes between two types of high-level healthcare role models:

1. Structural Roles
2. Functional Roles
3. Structural Roles⁸ place people in the organizational hierarchy as belonging to categories of healthcare personnel warranting differing levels of access to healthcare information. Structural

⁷ ASTM International E1986 lists healthcare roles for which access controls are warranted. These “enterprise roles” are referred to here as structural roles.

⁸ ASTM International E1986 list healthcare structural roles for which access controls are warranted.



roles allow a user to participate in the organization's workflow (e.g., tasks) by job, title, or position. Some structural role examples include: Physician, Pharmacist, Registered Nurse Supervisor, and Ward Clerk or Unit Secretary. Consumer privacy policy applied to structural roles constrains the actions that may be allowed to persons possessing the specified structural role attribute.

Functional Roles consist of all the permissions on health information system objects needed to perform a task. Functional roles define what authorizations are needed by an entity to access protected health information system (information technology) resources. Functional role names associate groups of permissions for convenience when assigning to users. A user may be assigned one or more functional roles, and thereby be assigned all of the permissions associated with a corresponding healthcare workflow. Permissions will ultimately be used to set the system operations (create, read, update, delete, etc.) needed to access Service Provider objects and functions.

Figure 3-3 Role Structure (Adapted from ANSI INCITS Role Model)⁹

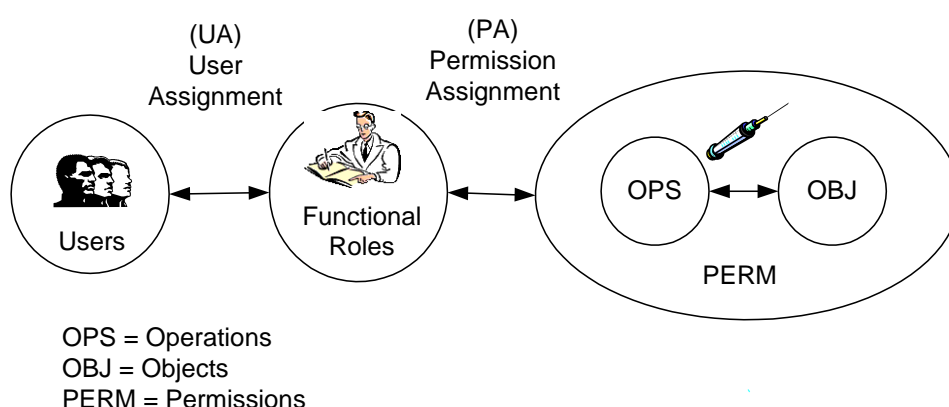


Figure 3-3 illustrates the Functional Role, Permission, and Operation and Object relationships. This figure is an adaptation of the NIST Core RBAC reference model. Further concepts include sessions/session roles, Hierarchical RBAC and Constrained RBAC which are topics beyond the scope of this document.

Permissions are defined by operations (create, read, update, and delete) on specific underlying health system information resources (objects). Some permissions include:

- Creating entries in laboratory results tables
- Certifying (signing) laboratory results entries
- Creating entries in patient orders tables
- Creating, reading, or updating patient allergy information

Consumer privacy policy applied to functional roles constrains the actions that may be performed on specified objects (e.g. constrains permissions granted to an entity).

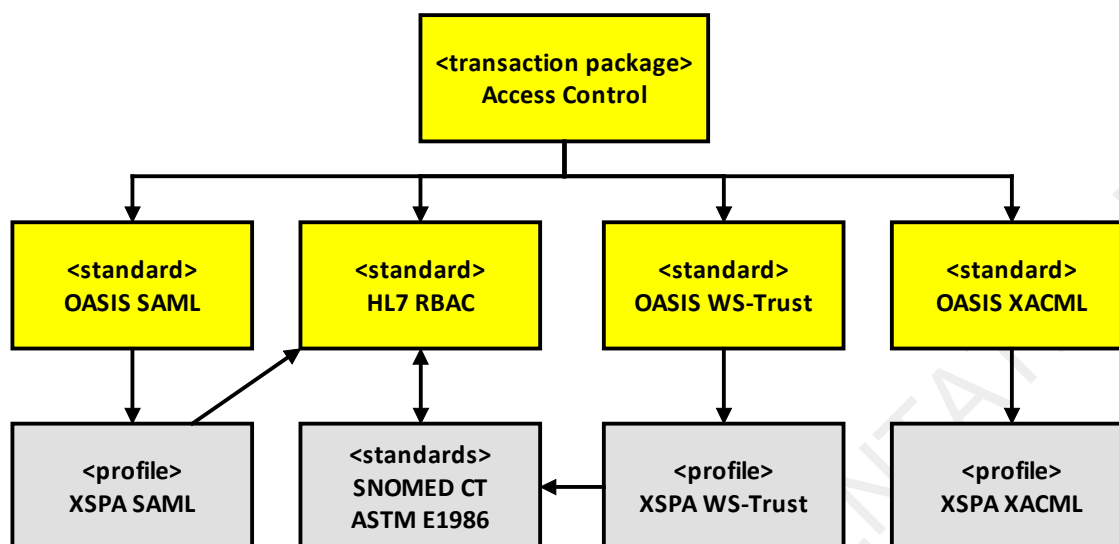
3.5 DESCRIPTION OF UNDERLYING STANDARDS

Figure 3-4 illustrates the selected standards, OASIS SAML, OASIS WS-Trust, and OASIS XACML, HL7 RBAC Healthcare Permissions Catalog (HL7 RBAC), and the relationships to the road mapped informative standards that are discussed in Section 2.1.2.

⁹ ANSI INCITS 359-2004 Role Based Access Control



Figure 3-4 Access Control Standards



The following sections provide further descriptions for the underlying standards that are described within this construct specification.

3.5.1 SAML

SAML attribute assertions and protocols form the core mechanism for exchanging access control information. Currently, the OASIS Cross Enterprise Security and Privacy Authorization (XSPA) SAML profile (U.S. Realm) is on track to become an OASIS standard. This Profile provides key vocabulary and value sets required to achieve interoperability as specified by this Transaction Package and will be included as a normative standard in future versions.

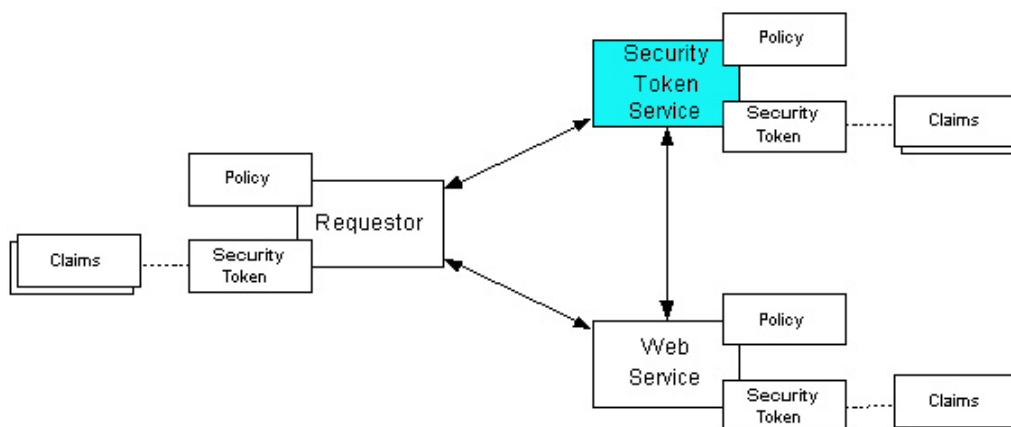
3.5.2 WS-TRUST

WS-Trust claims and protocols form a second core mechanism for exchanging Access Control information. Currently, the OASIS Cross Enterprise Security and Privacy Authorization (XSPA) WS-Trust profile (U.S. Realm) is on track to become an OASIS standard. This Profile provides key vocabulary and value sets required to achieve interoperability as specified by this and will be included as a normative standard in future versions.

Figure 3-5 illustrates the general WS-Trust security model involving claims, policies, and security tokens. The arrows indicate possible interaction paths between interfaces. The “Requestor” interface is mapped to the Service User interface in Table 2-1 Interfaces, and the “Web Service” interface maps to the Service Provider interface. The “Security Token Service” is exposed as a component of the Access Control Service. This model supports authorization specific models such as identity-based authorization, access control lists, and capabilities-based authorization including role-based access control (RBAC).



Figure 3-5 WS-Trust Security Model

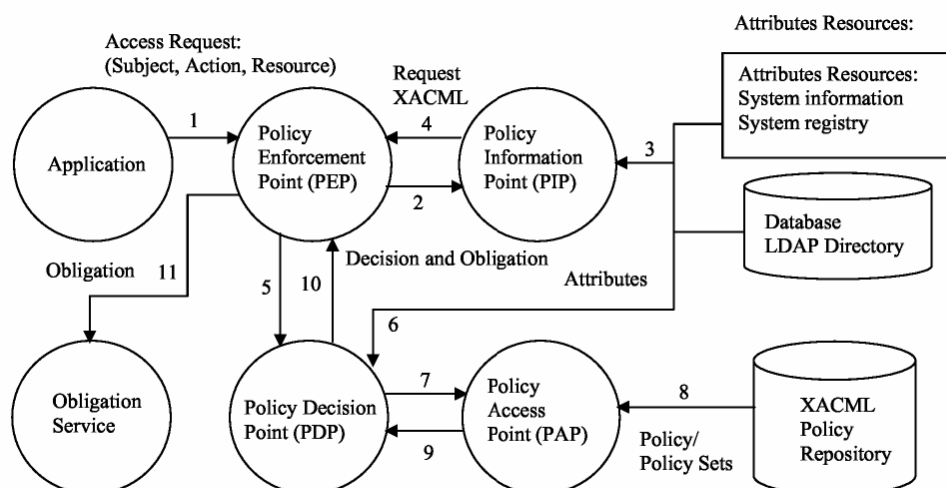


3.5.3 XACML

XACML forms a core mechanism for expressing security and privacy policy and for making and enforcing access control decisions based upon evaluating access control information. OASIS Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of XACML v2.0 for Healthcare Version 1.0," November 2009 (U.S. Realm) provides key vocabulary and value sets required to achieve interoperability of Access Control services within enterprises that choose to implement the OASIS model interoperable with the XSPA SAML Profile.

The OASIS XACML specification also broadly defines the components engaged in authorization interactions. These components are shown in the figure below. The "Application" interface maps to the Service Provider technical interface defined in Table 2-2. The remaining components are collectively considered part of the Access Control Service, which together with the WS-Trust Security Token Service define core capabilities of any Access Control Service technical interface. The specification of these components as part of an enterprise specific solution is out of scope of this Transaction Package.

Figure 3-6 OASIS XACML Components¹⁰



¹⁰ Source for Figure 3-6: NIST Interagency Report 7316 Assessment of Access Control Systems
Figure 2 XACML Architecture



There are two primary components: the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP). The workflow is as follows:

1. The PEP constructs the request based on the user's attributes, the resource requested, the action specified, and other situation-dependent information (e.g., purpose of use, roles, constraints and patient consent directives) through the Policy Information Point (PIP)
2. The PDP receives the constructed request, compares it with the applicable policy and system state through the Policy Administration Point (PAP), and then returns one of the replies specified above to the PEP
3. The PEP then allows or denies access to the resource

3.5.4 WS-FEDERATION

WS-Federation provides future capabilities for allowing authorized access to resources in one security domain to be provided to entities managed in another security domain. A fundamental goal of WS-Federation is to simplify the development of federated services through cross-realm communication and management of Federation Services by re-using the WS-Trust Security Token Service model and protocol. This construct recommends the use of WS-Federation as a means of allowing authorized access to resources in one security domain to be provided to entities managed in another security domain. WS-Federation defines mechanisms for:

- Brokering of identity
- Attribute discovery and retrieval
- Authentication and authorization claims between federation partners
- Protection of the privacy of claims across organizational boundaries

WS-Federation is currently on track to become an OASIS standard. WS-Federation is considered to be an extension of both WS-Security and WS-Trust. The documentation published by the OASIS WS-Federation TC describes these relationships and the services provided through WS-Federation in detail.

3.5.5 OTHER STANDARDS

All Profiles used in this construct use the same base standards of HL7 RBAC, SNOMED CT, and ASTM International E1986 to convey interoperable authorization information. ANSI INCITS provides a standardized framework and API for Role Based Access Control. ASTM International E2595 PMI provides guidelines for areas of consideration in implementing a privilege management infrastructure. ASTM International E1986 presents the structural roles described in ASTM International E2595 PMI. HL7 RBAC presents the healthcare permissions supporting fine-grained functional roles described in ASTM International E2595 required to access Service Provider functions and data.

The OASIS U.S. Realm XSPA Profiles of SAML (and, WS-Trust once adopted) provides the specifications for exchanging interoperable Access Control information. For enterprises implementing XACML, the OASIS U.S. Realm XSPA XACML Profile provides a recommended specification for expressing security Access Control information within an enterprise.



4.0 CHANGE HISTORY

The following sections provide the details of updates made to this document.

4.1 OCTOBER 5, 2007

The changes in this cycle address the following comments received during the Public Comment and Inspection Testing period (July 23, 2006 - August 17, 2007):

- 272, 714, 869, 874, 877, 883, 887, 890, 892, 896, 899, 900, 902, 904, 982, 984, 1196, 1197, 1228, 1229, 1230, 1231, 1243, 1262, 1263, 1264, 1265, 1266

4.2 OCTOBER 15, 2007

Upon approval by the HITSP Panel on October 15, 2007, this document has been moved to Version 1.1. This document is now Released for Implementation.

4.3 JULY 11, 2008

This document has been updated to reflect changes which are editorial in nature. This document has been moved to Version 1.1.1

- Interface names have been corrected to more accurately reflect the corresponding names in the referenced Implementation Specification.
- Updated to place standards into 3 categories: Regulatory, Selected, and Informative References.
- Updated name/description of standard for ASTM International PMI, and HL7 v3 RBAC

4.4 AUGUST 20, 2008

This document has been modified to reflect the updated HITSP approach to categorizing standards as Regulatory Guidance, Selected Standards, and Informative References.

The following standard was added as an informative reference:

- Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile Added to Informative Reference Table

4.5 AUGUST 27, 2008

Upon approval by the HITSP Panel on August 27, 2008, this document is now Released for Implementation.

4.6 DECEMBER 10, 2008

Minor editorial changes were made to this construct.

This Transaction Package has been updated with editorial and minor updates of a technical nature as follows:

4.6.1 SECTION 1 UPDATES

The following technical changes have been made to Section 1.0:

- Moved overview text that was more detailed from Section 1.1 to Section 2.1



- Security and Privacy Technical Note no longer has glossary or description of application of Security and Privacy constructs to HITSP Interoperability Specification's, so updated Table 1-1 with this information

4.6.2 SECTION 2 UPDATES

The following technical changes have been made to Section 2.0:

- Table 2-1 Interfaces
 - Provided further clarification on the standards for which the interfaces will be used
 - Corrected the optionality of the interfaces to indicate that at least one of the Service User or Service Provider interfaces is required to be implemented
- Section 2.1.2 Interface Interactions
 - Added high level overview narrative and Figure 2-1 to provide further details on the typical access control interactions between parties in the exchange of health information
 - Reorganized the section narrative to provide clarity by moving supplemental, supporting material from Section 2.1.2 into the Appendix in Section 3.0
 - Edited the narrative to improve readability and consistency
- Table 2-2 Context
 - Minor edits to the pre-conditions to improve readability
- Table 2-8 Selected Standards
 - Moved the standard reference for OASIS WS-Federation from Table 2-8 Selected Standards to Table 2-9 Informative Reference Standards
 - Updated the IHE ATNA Profile reference to point to Revision 5.0 or later
- Section 2.3.3 Informative Reference Standards
 - Added informative references to the OASIS XSPA SAML, OASIS XSPA WS-Trust, and OASIS XSPA XACML profiles as road mapped references

4.7 DECEMBER 18, 2008

Upon approval by the HITSP Panel on December 18, 2008, this document is now Released for Implementation.

4.8 JUNE 30, 2009

Minor editorial changes were made to the document, including the UML (Unified Modeling Language) diagrams. Removed boilerplate text for simplification. The term "actor" was replaced with "interface".

4.9 JULY 8, 2009

Upon approval by the HITSP Panel on July 8, 2009, this document is now Released for Implementation.

4.10 NOVEMBER 9, 2009

The specification has been updated as follows:

- Included Figure 2-2 Component Relations in Access Control Interfaces illustrating Access Control interfaces
- Adopted OASIS Standard, "Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of Security Assertion Markup Language (SAML) for Healthcare Version 1.0," November 2009
- Adopted American Society for Testing and Materials ASTM International #E1986 -98 (2009) Standard Guide for Information Access Privileges to Health Information



- Updated Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008 to R2-2009, Release 2, October 2009 pending ANSI acceptance
- Minor edits to improve clarity in pre-conditions and text throughout document

4.11 JANUARY 18, 2010

Updated to the HITSP Transaction Package Template Version 2.7.

The specification has been updated with editorial and minor updates of a technical nature as follows:

- ASTM International (2005) version removed from informative reference standards table – it should have been removed during the November release when the 2009 version was adopted as a selected, normative standard
- OASIS eXtensible Access Control Markup Language (XACML), February 2005, was incorrectly published as both a selected standard and an informative reference. It is a previously selected standard, and should not have been published as an informative reference. The listing in the informative reference table has been removed
- Comment 9521 and 9522: XSPA-SAML was selected as a normative standard, and should have been placed in the “selected standards” table, but was incorrectly added to the “informative reference” standard table in the November release. These errors have been corrected
- Comment 8952 was addressed. Explanatory text regarding SOAP and HITSP/TN907 was added to Section 2.1
- Comment 9059 was addressed. “Service Consumer” was changed to “Service User” throughout
- Comment 9060 was addressed. Text in Table 4-1 was amended
- Comment 9519 was addressed. Section 2.1.1 (missing paragraph) was corrected
- Comment 9520 was addressed. The bulleted list is corrected
- Comment 9523 was addressed. Typographical updates were made as requested

The full text of the comments along with the Technical Committee’s disposition can be reviewed on the [HITSP Public Web Site](#).

4.12 JANUARY 25, 2010

Upon approval by the HITSP Panel on January 25, 2010, this document is now Released for Implementation.

