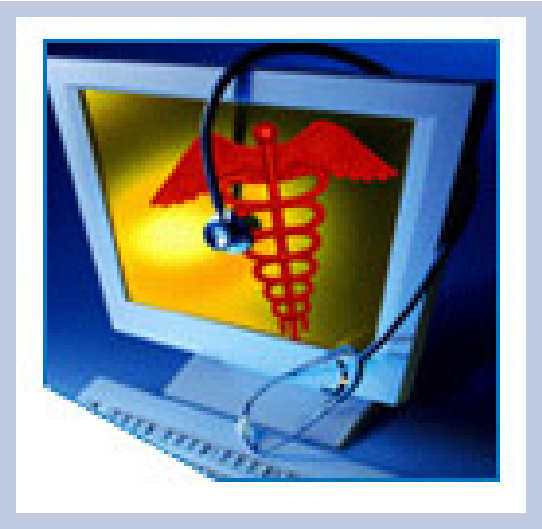
August 27, 2008
Version 1.2

HITSP Access Control Transaction Package

HITSP/TP20



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
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

TABLE OF CONTENTS

FIGURES AND TABLES

1.0 INTRODUCTION

As an introduction to the HITSP Access Control Transaction Package, this section provides a high level overview of the information sharing scenario(s) enabled by following this specification, provides a document map of the construct relationships for the HITSP specification, acknowledges the copyright protections that pertain, and provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.0 Transaction Package Definition.

1.1 OVERVIEW

This section describes the contents of this specification and provides a high level definition of this Transaction Package and background information about the underlying Transactions and Components that the Transaction Package is based on.

The Access Control Transaction Package provides the mechanism to administer 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 or 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.

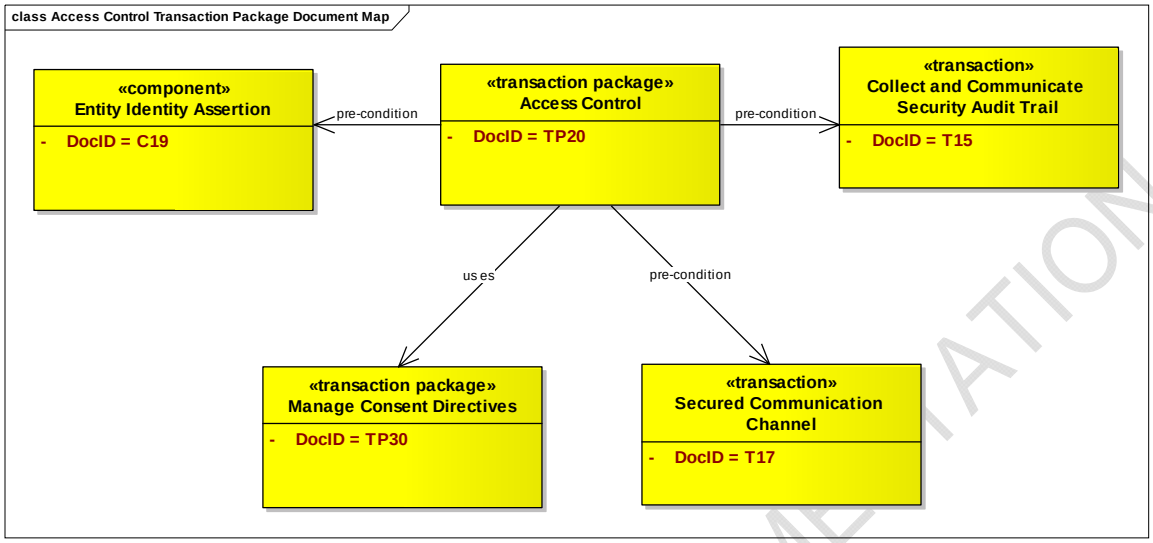
There are 2 actions that must be completed in order to effectively use this construct:

1. Deciding the rules to 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. When you instantiate the rules, they are written in terms that the system can understand and get enforced

1.2 TRANSACTION PACKAGE DOCUMENT MAP

Each HITSP specification describes a suite of constructs that, taken as a whole, define how to integrate and constrain existing standards and specifications that will satisfy the requirements for the HITSP construct. There are four types of HITSP constructs called Interoperability Specifications (IS), Transaction Packages (TP), Transactions (T), and Components (C). Interoperability Specifications define the context(s) in which any other HITSP construct may be used. The current Access Control Transaction Package specification is used with other constructs to meet the requirements of one or more ISs. Review Section 1.2 Interoperability Specification Document Map from the relevant IS to better understand the context, dependencies, and relationships between the constructs used to meet the IS requirements. The Document Map in Figure 1.2-1 depicts how this construct integrates and constrains HITSP constructs to support the information exchange, within the defined context of this document. Implementers should read the documents that describe the constructs depicted in the diagram for their details and specific uses.

Figure 1.2-1 Access Control Transaction Package Document Map



1.3 COPYRIGHT PERMISSIONS

COPYRIGHT NOTICE

OASIS materials used in this document have been extracted from relevant copyrighted materials with permission of the Organization for the Advancement of Structured Information Standards (OASIS). Copies of this standard are available from OASIS at www.oasis-open.org.

1.4 REFERENCE DOCUMENTS

This section provides a list of key reference documents and background material. If you are already familiar with this information, proceed to Section 2.

A list of key reference documents and background material is provided in the table below. These documents can be retrieved from the www.hitsp.org Web Site.

Table 1.4-1 Reference Documents

Reference Document	Document Description
HITSP Interoperability Specification Overview	Provides background information about the HITSP and its role in the overall U.S. efforts to realize large scale interoperability of health information. The document also provides a description of the HITSP process for healthcare standards harmonization and explains how to use the Interoperability Specifications and other related documents to inform your health IT product development or product refinement.
HITSP Conventions List	Describes the conventions that are used to convey the full descriptions and usage of standards in the HITSP specifications
HITSP Acronyms List	Lists and defines the acronyms used in this document
HITSP Glossary	Provides definitions for relevant terms used by HITSP documents
HITSP Harmonization Framework	Describes the current framework within which the Interoperability Specifications are built
TN900 - Security and Privacy Technical Note	Developed as a reference document to provide the overall context for use of the HITSP Security and Privacy constructs. It includes the following: • The scope, reference policy background, and Security and Privacy principles used in the development of the constructs • A detailed description and schematics of the conceptual relationship between the Security and Privacy constructs • A mapping of existing standards and constructs to be used in meeting the stated requirements of the AHIC Use Cases • A list of identified gaps and the recommended approaches to resolving those gaps • A roadmap for how the Security and Privacy constructs will evolve and eventually align with other HITSP Interoperability Specifications • A conceptual framework for Security and Privacy management, including reference information on privacy policies, risk assessment, and risk management • A glossary of terms used in all the Security and Privacy construct documents • A description of the application of the Security and Privacy constructs to the HITSP Interoperability Specifications for the three initial AHIC Use Cases – Biosurveillance, Electronic Health Records - Laboratory Results Reporting, and Consumer Empowerment HITSP will periodically update this Technical Note as required by the introduction of new contexts for use.

2.0 TRANSACTION PACKAGE DEFINITION

Transaction Packages define how two or more Transactions are used to support a stand-alone information exchange within a defined context between two or more systems.

2.1 CONTEXT OVERVIEW

This section provides a general description of the Transaction Package. It includes a detailed definition of the Transaction Package and the reason for its use. It also provides all the necessary background information that further describes the context in which the Transaction Package is needed, and the independent Transactions and Components that the Transaction Package is based on.

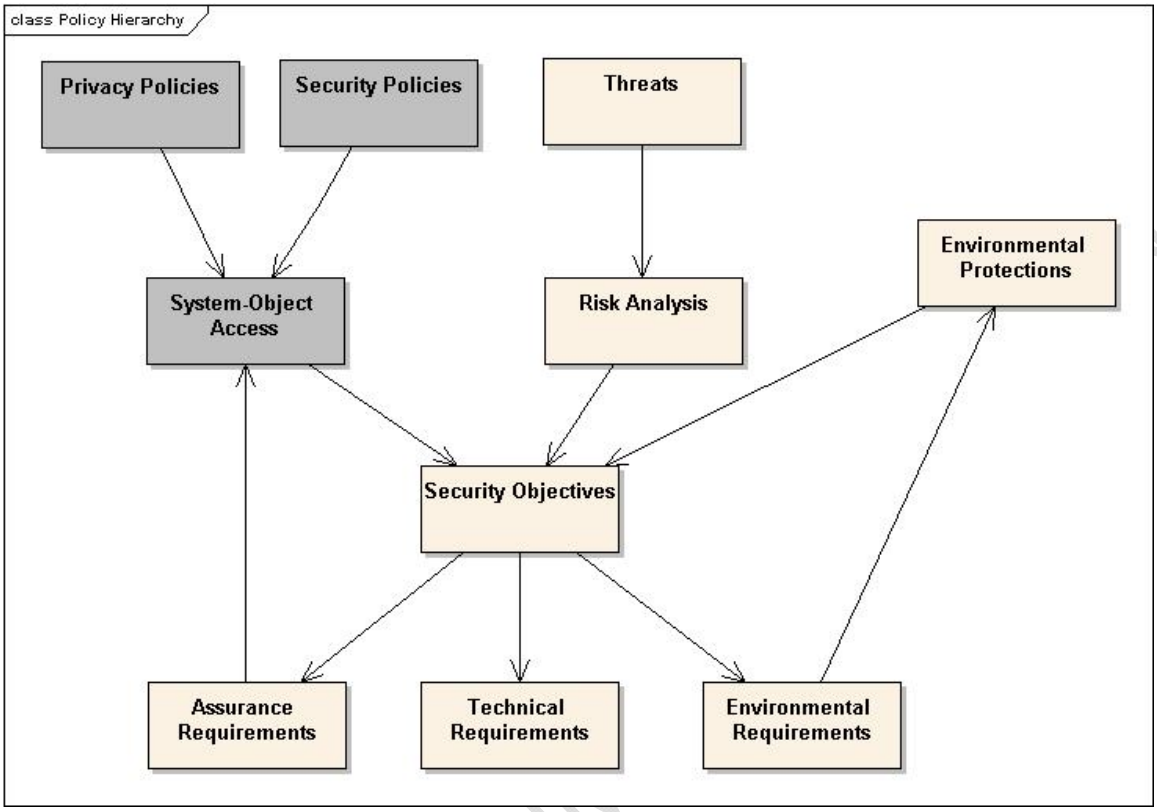
The following are the requirements derived from the AHIC Use Cases that apply to this construct:

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 bypass is enforced (Emergency access)
4. User data are located by an entity with the ability (privileges) to search across systems
5. Protected data are accessed based on access control decisions, information attributes for subjects, resources, actions or the environment
6. Protected data are modified, updated or corrected only by authenticated, 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
10. Protected data – 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 enforcement of the resulting merged set of policies that are used to determine if access to system resources and functions are to be authorized.

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.

Figure 2.1-1 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 &2 provides the framework and models for security management used in this package.

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 impose 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 possible types of access control information used in this package.

WS-Trust OVERVIEW

This construct specifies the use of WS-Trust as a token-type agnostic model for a security token service (STS) that provides token management capabilities including:

- Requesting
- Issuing
- Renewing
- Canceling
- Validating

Any number of tokens is possible, including Kerberos, PW, X509 or proprietary.

WS-Federation OVERVIEW

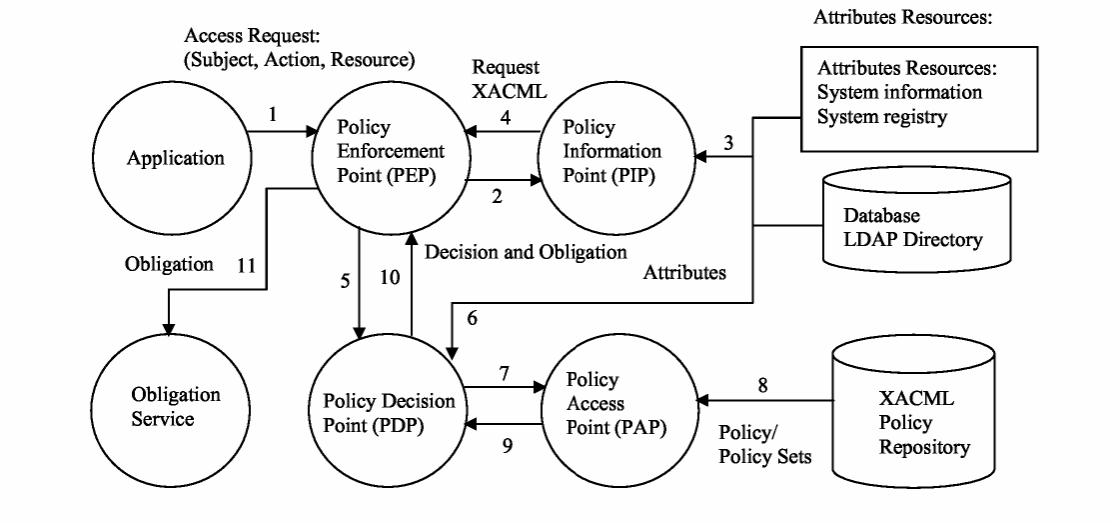
This construct specifies the use of WS-Federation as a means of allowing authorized access to resources in one security domain to be provided to entities managed in another security domain. WS-Federation defines mechanisms as extensions to WS-Trust for:

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

OASIS XACML OVERVIEW

This construct specifies the use of OASIS XACML as a means to express security and privacy policy and obligations. While the OASIS XACML specification completely describes these interactions, a brief overview is provided here describing the interactions between various components. These interactions are essential to the operation of this construct and together with the WS-Trust Security Token Service and WS-Federation define the capabilities of this construct's "Access Control Service".

Figure 2.1-2 OASIS XACML Components[1]



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. Since it is based on XML, it is, as its name suggests, easily extensible. 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

XACML's standardized architecture shown in figure 2.1-2 for this decision-making uses two primary components: the Policy Enforcement Point (PEP) and the Policy Decision Point (PDP). The PEP constructs the request based on the user's attributes, the resource requested, the action specified, and other situation-dependent information through the Policy Implementation Point (PIP). The PDP receives

[1] Source for Figure 2.1-2: NIST Interagency Report 7316 Assessment of Access Control Systems Figure 2 XACML Architecture

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. The PEP then allows or denies access to the resource. The PEP and PDP components may be embedded within a single application or may be distributed across a network.

To make the PEP and PDP work, XACML provides a policy set, which is a container that holds either a policy or other policy sets, plus (possibly) links to other policies. Each individual policy is stated using a set of rules. XACML also includes methods for combining these policies and policy sets, allowing some to override others. This is necessary because the policies may overlap or conflict. Possible conflicts are resolved through policy-combining algorithms. For example, a simple policy-combining algorithm is "Deny Overrides," which causes the final decision to be Deny if any policy results in Deny. Conversely, other rules could be established to allow an action if any of a set of policies results in Allow. XACML includes standard policy-combining algorithms, and developers can create their own as well.

Transferring XACML Policies

Policies may need to be transferred from one entity to another in a Privilege Management Infrastructure or as part of this construct. Some of the situations where this is required are:

1. A PDP evaluates a policy that references other policies by name. The other policies must draw from a Policy Administration Point (PAP) when required for evaluation
2. A PDP may need to obtain its "root" policy from the enterprise PAP as part of configuration
3. A resource may be transferred between security domains, and the source domain may transfer a policy for protection of the resource that the destination domain is responsible for enforcing
4. Multiple sites may need to use common policies, even though their PDPs are local for performance reasons. These policies need to be transferred from the central Policy Administration Point to each site's PDP

While XACML defines a policy language, it is designed to be one component in an overall authorization system. It relies on other components to provide mechanisms for verifying that policy instances were issued by a trusted Policy Administration Point, for protecting the integrity and confidentiality of instances of policies, and for protocols used to query for and respond with policy instances. XACML has been integrated with the OASIS Security Assertion Markup Language (SAML) Version 2.0 as one way of providing these necessary functions. SAML may be used with XACML to protect Access Control Information attributes as well as policies.

2.1.1 TRANSACTION PACKAGE CONSTRAINTS

This section describes the constraints that limit the context in which the Transaction Package construct may be used. A constraint describes a rule that limits the use of the actors, actions or data within the given context, or to which the interactions must conform to be used within the described context. It is a description of the limits and scope of the interactions and can describe actions or events that are not part of the initial definition for the context.

Table 2.1.1-1 Transaction Package Constraints

Constraint
Entities must be members of defined information domains under the authorization control of a defined set of polices.
The Transaction Package applies to any circumstance in which authorizations need to be adjudicated for access to protected information.

2.1.2 TECHNICAL ACTORS

This section describes the technical actors that need to be integrated in order to meet the interoperability requirements for this Transaction Package. A Technical Actor represents an entity internal to a software application, which is engaged in one or more specific Transactions to support a specific aspect of a real world information interchange (e.g., set of message exchanges). The table below lists the technical actors involved, the relevant definition of their roles, and an indication of their requirements for the Transaction Package.

Table 2.1.2-1 Technical Actors

Actor	Description	Used in Component/ Composite Standard	Required = R Optional = O Conditional = C
Service User [formerly 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 transaction. Any Service User may also be a Service Provider.	WS-Trust, WS-Federation, XACML, SAML, RBAC	R
Access Control Service (ACS) [formerly User Access Control Service (UACS]	The Access Control Service is the enterprise security service that supports and implements user-side and service side access control capabilities. This service would be utilized by the Service User, and/or Service Provider.	WS-Trust, WS-Federation, XACML, SAML, RBAC	R
Service Provider (SP)	The service provider represents the system providing a protected resource and relies on the provided security service.	WS-Trust, WS-Federation, XACML, SAML, RBAC	R

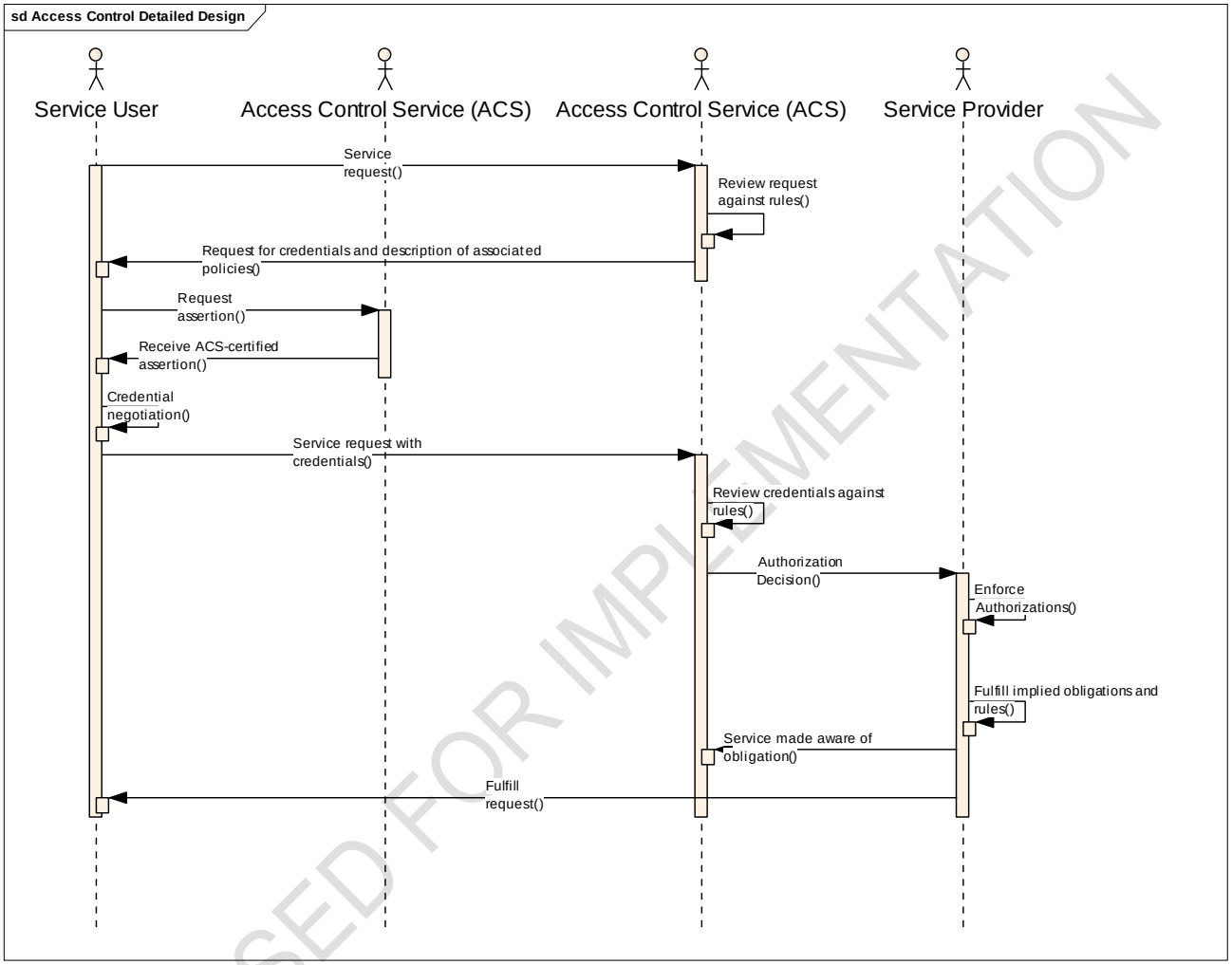
Note that the Access Control Service Actor is the normative name for the User Access Control Service and Service Provider Access Control Service actors, and there may be both local and remote versions of these actors.

2.1.3 ACTOR INTERACTIONS

This section uses a Unified Modeling Language (UML) workflow diagram to depict the business and technical actors, the relevant events or actions in which they are involved, and a mapping to the Transactions, and Components that encapsulate the defined events/actions. It describes the underlying events that fulfill the Transaction Package, the sequence and timing of the events, and the specific actors

involved. Process flow diagrams are also provided to illustrate the process relationships. A description of the UML diagram is also provided below the diagram.

Figure 2.1.3-1 Access Control Actor Interaction Diagram



The pre-conditions that need to be in place at the beginning of this construct are specified in Table 2.1.4-1.

Interoperability events:

The Access Control Actor Interaction diagram shows the basic process flows for the access control Transaction Package. The standards that frame the interaction are WS-Trust, WS-Federation, SAML, XACML, and ATNA through the HITSP/T15 construct. The process flows are:

1. The user initiates the service request (including token claims)

2. The service request is intercepted by the Service Provider 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
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 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 consents, etc.)
5. The user negotiates/requests needed credentials from the Access Control Service (ACS) or other source
6. The user responds to the Service Provider ACS credential request with a request that includes the needed claims (tokens)
7. The Service Provider ACS verifies the claims/assertions provided against the run-time policies for access. As before, if the Service Provider 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 ACS forwards the request and authorization decision to the Service Provider. The exact nature of this exchange may vary. The Service Provider ACS also communicates any obligations associated with this request to the Service Provider
9. The Service Provider receives the service request, the Service Provider ACS decision and any obligations. If additional access decision support is needed, then the Service Provider 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 2.1.5-1 below.

2.1.3.1 Example: Application of Access Control to EHR-Lab Use Case Event - 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 AHIC Harmonized Use Case for Electronic Health Records (Laboratory Results Reporting) (EHR-Lab), applied to the access control models described above.

The following pre-conditions are directly extracted from the EHR-Laboratory Results Reporting AHIC Use Case:

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 Component. 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 for the Access Control construct also need to be in place and are described in Table 2.1.4-1. Specifically, PAPs write policies and policy sets and make them available to the 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 Transaction Package 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 HITSP Access Control Transaction Package enforces those policies.

Access Control Context

Scenario Condition: Provider access to patient health information is verified in accordance with the consumer consent. (HITSP/TP30)

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 allows 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 here for example, includes review permissions of Laboratory Orders.

Table 2.1.3-1 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 shown in Figure 2.1-1 are determined using the HISTP/TP30 construct for 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 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).

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.

Use Case Condition: Patient consent directives (and security policies) are enforced to allow or block access to patient health information (line spacing)

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 (HITSP/T15), 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 for the above EHR-Lab event are specified in the Post-Conditions Table 2.1.5-1. 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 the Required Outputs Table 2.1.5.1-1.

2.1.4 PRE-CONDITIONS

This section describes the necessary conditions that must be in place prior to the start of the workings of the Transaction Package. The pre-conditions are used to convey any conditions that must be true at the outset of a Transaction Package. They describe the context that must be established before the Transaction Package is executed. They are not however the triggers that initiate the Transaction Package. Where one or more pre-conditions are not met, the behavior of the Transaction Package should be considered uncertain.

Table 2.1.4-1 Pre-conditions

Pre-condition
Entities must have been identified and provisioned (credentials issued, privileges granted, etc.).
Privacy policies are identified and provisioned (consents, user preferences, etc.) in accordance with policy.
Domain defines appropriate vocabulary for policies.
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-existing Security and Privacy policies are provisioned to access control services.
Agreements regarding tokens, types, keys are negotiated in advance.
The capabilities and location of requested information/document repository services are known.
Secured channels are established as required by policy in accordance with HITSP/T17 - Secured Communication Channel.
Audit services are initialized in accordance with HITSP/T15 - Collect and Communicate Security Audit Trail.
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.
Requests for updates/appends to data by patients have been received and approved.
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, user profiles) is in place and supported by ACS and Authorization Mechanisms.
RBAC and role engineering, with identified structural and functional roles, is supported by ACS and Authorization Management.
Emergency access, with associated policies and authorizations, is supported by ACS and Authorization Management.
Mechanisms for making resource metadata known, including access polices have been established.
Recommended Future Pre-Conditions
Federated authorization is supported by standardized vocabulary for the expression of cross-enterprise security authorizations and is used by ACS and Authorization Management.
Federated obligation is supported by standardized vocabulary for the expression of cross-enterprise security and privacy obligations and is used by ACS and Authorization Management.

The following standards listed in Table 2.1, are used for satisfying these pre-conditions; ANSI INCITS provides a standardized framework and API for Role Based Access Control. ASTM PMI provides guidelines for areas of consideration in implementing a privilege management infrastructure. HL7 RBAC presents the healthcare permissions that may be assigned to licensed or certified healthcare providers. The ISO-10183 (ISO AC) standard specifies a general framework for the provision of access control. The

ISO PMAC standard supports the needs of healthcare information sharing across unaffiliated providers of healthcare, healthcare organizations, health insurance companies, their patients, staff members and trading partners. And the ISO SF Roles standard provides guidance for creating roles, by defining and describing some roles based upon European business models.

2.1.4.1 Process Triggers

This section describes the triggers, including actors and/or processes, which are necessary to start the Transaction Package. They can invoke an automatic or manual process or result that in turn starts off the Transaction Package. A trigger is not the same as a pre-condition that describes a context that needs to be in place at the start of the event.

Table 2.1.4.1-1 Process Triggers

Trigger
Request for protected resources, e.g., protected information, protected functionality, etc.

2.1.5 POST-CONDITIONS

This section provides an overview of the conditions or results that must occur at the end of the Transaction Package in order for the Transaction Package to be deemed successfully completed. This includes any required outputs from the Transaction Package, or specific actor states.

This construct should provide the mechanisms to protect any piece of information needing protection, even if it doesn't have anything to do with a patient. If non-patient information is protected, there is not a need to call to the privacy operations. The security system can enforce any rule that is input – whether it is a security or privacy rule.. Systems are currently designed such that the service obligation is fulfilled at the next step. There is a need to make sure that the policy rules are considered prior to the access control's provision of the data. Essentially, this mechanism can work on any set of policies that are provided. The post-conditions are framed by the ISO AC, WS-Federation, and XACML standards.

Table 2.1.5-1 Post-conditions

Post-conditions
Access is authorized or denied. If access is permitted, then the PEP permits access to the resource; otherwise, it denies access.
Issued credentials that are no longer required are cleaned up.
Any requirements and obligations on enterprise systems are fulfilled (e.g. audit events are recorded).

2.1.5.1 Required Outputs

This section identifies the required outputs that must be produced at the end of the Transaction Package in order for the Transaction Package to be deemed successfully completed. This includes the format and usage of the required output.

Table 2.1.5.1-1 Required Outputs

Output	Format/Usage
Audit events are recorded and alerts communicated.	Specified in HITSP/T15 – Collect and Communicate 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".

2.1.6 DATA FLOWS

This section describes the basic data flows that are supported by this Transaction Package. It also describes the format of the data, the data sources, and the relevant actors involved in the successful flow of data for the Transaction Package. Any prevailing pre and post-conditions are identified, as well as the purpose of each data post-condition associated with each Transaction Package. Any data that need to be made available to particular actors are highlighted, as well as the conditions and processes that will use the data to achieve the stated post-conditions.

Data flows are portrayed for this Transaction Package in Figure 2.1.3-1 Access Control Actor Interaction Diagram.

2.2 LIST OF HITSP CONSTRUCTS

The following list of constructs and their definitions are used by the Transaction Package specification.

Table 2.2-1 List of Constructs

Construct Name	Description	Event/Action Code	Content/Use
HITSP/T15 - Collect and Communicate Security Audit Trail	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.	N/A	Happens before the point where the enforcement decision is made, and at the point where service decision is fulfilled.
HITSP/TP30 - Manage Consent Directives	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)	N/A	HITSP/TP30 is the engine to create an authoritative set of policies (consent directives), that this construct then enforces

2.2.1 CONSTRUCT DEPENDENCIES

The following table shows a list of constructs with their existing dependencies. Dependencies usually exist when there are some additional pre-requisites for a specific Transaction specification.

Table 2.2.1-1 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

This section describes the constraints that further limit the constructs that are used by this Transaction Package.

Table 2.2.2-1 Additional Constraints on Required Constructs

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

2.3 STANDARDS

It is important to understand that the standards selected here are within the context of the specific Use Case requirements and do not necessarily reflect selection in other contexts. The standards used by this Transaction Package specification fall into the following categories:

- Regulatory guidance is a legal or other authoritative declaration that HITSP must abide by in standards selection (see Section 2.3.1)
- Selected standards are necessary for interoperability. These are standards that are used to meet information exchange requirements of associated constructs. For example, they are used to realize direct information exchange, to provide the transport mechanism, to specify the content, or to address security (see Section 2.3.2)
- Informative reference standards provide additional background information or guidance, and are not required for interoperability. These standards are not required to implement the Transaction Package specification (see Section 2.3.3)

2.3.1 REGULATORY GUIDANCE

The following table provides a list of legal or other authoritative guidelines that HITSP must abide by, or has agreed to use as guidance in the selection of standards. Note that only the referenced sections of the regulations are relevant to this Transaction Package specification.

Table 2.3.1-1 Regulatory Guidance

Standard	Description
No applicable regulatory standards	

2.3.2 SELECTED STANDARDS

The following table provides a list of standards that are used to meet information exchange requirements of the Transaction Package specification, and a detailed description of each standard.

Table 2.3.2-1 Selected Standards

Standard	Description
Health Level Seven (HL7) V3 RBAC, R1-2008, HL7 Version 3 Standard: Role Based Access Control (RBAC) Healthcare Permissions Catalog, Release 1, February 2008	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) v2.0 OASIS Standard; ITU-T X.1141	SA 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) 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 Toke 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) WS-Federation Web Services Federation Language (WS- Federation), Version 1.1, December 2006	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) 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 XCML 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

2.3.3 INFORMATIVE REFERENCE STANDARDS

The following table lists standards that provide additional background information or guidance; however, they are not required for the implementation of the Transaction Package specification.

Table 2.3.3-1 Informative Reference Standards

Standard Name	Description/Usage
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 http://www.ansi.org
American Society for Testing and Materials (ASTM) 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
Integrating the Healthcare Enterprise (IHE) IT Infrastructure Technical Framework (ITI-TF) Revision 4.0, Audit Trail and Node Authentication (ATNA) Integration Profile	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 actor specific requirements. The latest version of the IHE Technical Framework is available at www.ihe.net

Standard Name	Description/Usage
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
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 actors. 2. Directory services: structural roles are usefully recorded within directories of health care 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 www.iso.org

3.0 TECHNICAL IMPLEMENTATION

3.1 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.

3.1.1 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 be constrained as specified in table 2.1.1-1, and implement all of the required actors from table 2.1.2-1, 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 with which this construct is associated.

3.1.2 CONFORMANCE SCOPING, SUBSETTING AND OPTIONS

A HITSP Interoperability Specification must be implemented in its entirety for an implementation to claim conformance to the specification. HITSP may define the permissibility for actor 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 to claim conformance.

4.0 CHANGE HISTORY

The following sections provide the history of changes 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

The full text of the comments along with the Technical Committee's disposition can be reviewed on the HITSP Public Web Site.

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

- Technical actor 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 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.