V3_PSAF_R1_N3_2019SEP

# HL7 Version 3 Standard: Privacy and Security Architecture Framework Release 1

## Volume 2: Trust Framework for Federated Authorization Behavioral Model

## HL7 Normative Ballot

September 2019

**Sponsored by:**
**Security Work Group**
**Community Based Care and Privacy Work Group**

 

## Important Note to September 2019 Ballot Voters

The September 2019 Privacy and Security Framework (PSAF) ballot is a package containing all of the Volumes developed to date under the PSAF Project Scope Statement 914. See the September Ballot Announcement:

https://confluence.hl7.org/display/HL7/2019SEP+Announcement+of+Formation+of+Consensus+Groups

The Privacy and Security Architecture Framework (PSAF) is comprised of:

- Volumes 1 and 2, and the Informative Guidance document for Trust Framework for Federated Authorization conceptual and behavioral models (TF4FA), which passed normative ballot in May 2018. Being normative, it is not in scope for September 2019 ballot comments.
- Volume 3 Provenance, a conceptual model addressing topics needed for trustworthy information exchange, passed normative ballot in January 2019. It has been significantly restructured as a Domain Analysis Model (DAM) for the September 2019 ballot based on input from commenters and stakeholders. Volume 3 Provenance is in scope for September 2019 ballot comments.
- Volume 4 Audit, a conceptual model for the audit service interfaces. This document was approved as normative in January 2017 under the title HL7 Version 3 Standard: Privacy, Access and Security Services (PASS) - Healthcare Audit Services Conceptual Model, Release 1 (PI ID: 1264). However, the Security Work Group missed the publication deadline, so this volume was re-balloted and past normative during the May 2019 cycle. Being normative, it is not in scope for September 2019 ballot comments.
- The Security Work Group decided to combine all volumes into one ballot package to keep them moving in tandem through balloting, publication and potential reaffirmation.

As stated, only Volume 3 Provenance, is in scope for comments for September.

Inclusion of Volumes 1, 2, and the TF4FA Guide, and Volume 4 in the September PSAF ballot package also affords voters an opportunity to review the wider privacy and security context in which the Provenance DAM was developed, and to which it contributes a significant component.

# Acknowledgements


| TF4FA Contributor Table | |
|---|---|
| Mike Davis VHA Security Architect<br>Project; Authoring Lead<br>Publishing Facilitator | |
| Dave Silver, Principle Contributor<br>Electrosoft Inc. | Ioana Singureanu, Principle Contributor<br>Eversolve, LLC |
| **Sponsoring HL7 Security Work Group Co-chairs** | |
| Chris Shawn VHA<br>Project and Authoring Co-lead | Kathleen Connor Book Zurman Incorporated |
| Alexander Mense Fachhochschule Technikum Wien, Vienna. | John Moehrke By Light |
| Trish Williams<br>Professor of Digital Health Systems<br>Flinders University School of Computer | |
| **Co-sponsoring HL7 Community Based Collaborative Care [CBCC] Work Group Co-chairs** | |
| Suzanne Gonzales-Webb<br>Book Zurman Incorporated | Jim Kretz<br>Substance Abuse and Mental Health Services Administration [SAMHSA] |
| Johnathan Coleman<br>Security Risk Solutions | David Pyke<br>Ready Computing |

# Table of Contents

## List of Figures



## List of Tables




 

# List of Appendices




 

# PREFACE

This document is part of a series of interrelated documents that together comprise Health Level 7's emerging Trust Framework for Federated Authorization (TF4FA). The documents address core security topics from the perspective of enabling healthcare line-of-business interoperability for information exchange, and include:

- *TF4FA Volume 1*: presents a general architecture for creating a trusted relationship with a healthcare partner supporting policy derivation for security and privacy. This document provides a general conceptual overview of what defines interoperable authorized exchange and what is needed to achieve it.
- *This TF4FA Volume 2*: presents a more technical behavioral model describing logical interaction among Federated Authorization components.
- *TF4FA Guide*: presents an informative supplement that amplifies information contained in Volumes 1 and 2.

Further, as Figure 1: Elements for Establishing Trustworthy Interoperability illustrates, the document series illustrates the larger context of establishing trustworthy interoperability for information exchange. Figure 2 provides a slightly more detailed view of what each trust topic encompasses.

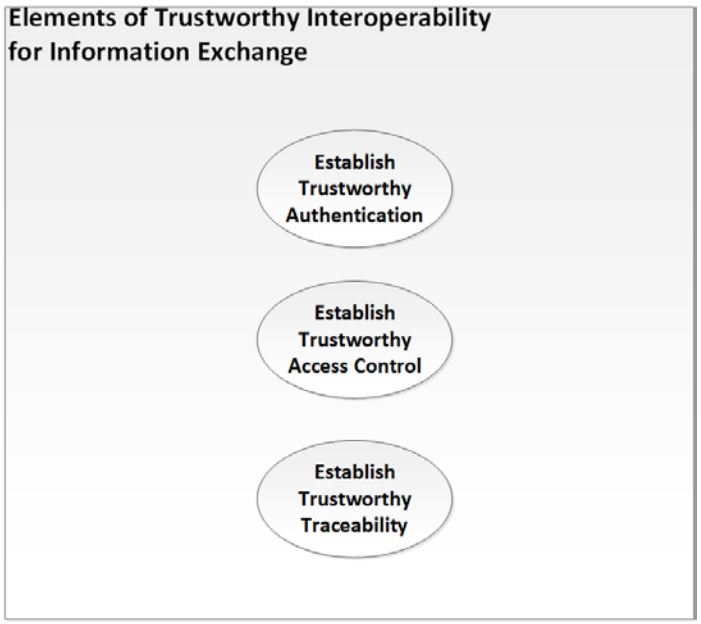


**Figure 1: Elements for Establishing Trustworthy Interoperability**

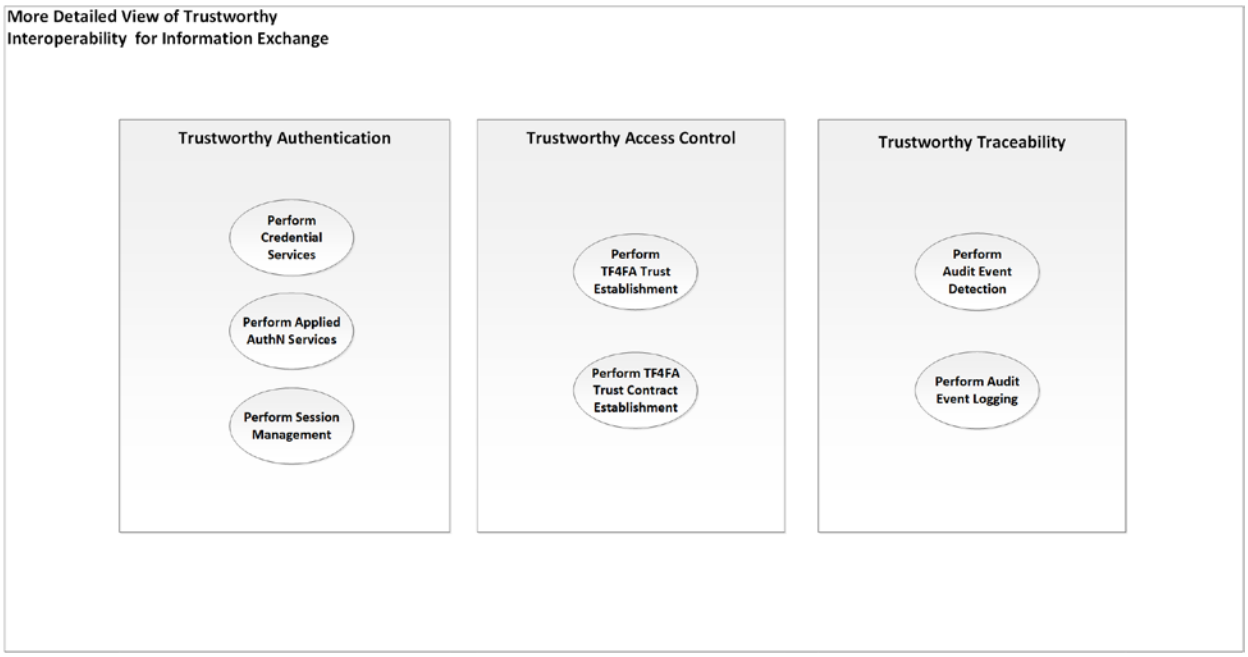


**Figure 2: More Detailed View of Establishing Trustworthy Interoperability**

# 1 INTRODUCTION (Informative)

The federated trust and authorization framework outlined in Volume 1 of this specification is based on trust derived between domains and manifested in computable trust contracts that make the derived business and technical operational rules legally binding between federation domain members. The trust contracts are derived by trust services, each of which derives a specific aspect of the trust contract or provides a supporting service.

- Federated Domain Model
- Information Model
- Trust Services Model

In the context of federated authorization, trust is the "circumstance existing between two entities whereby one entity makes the assumption that the other entity will behave exactly as the first entity expects" [ISO 22600-2]. In other words, trust defines the individual expectations in the context of the collection, processing, communication and use of personal information. It allows acceptance of risk and balancing privacy needs against benefits.

Typical access trust models are inherently at risk of improper handling and use of shared information because participating domains do not coordinate their local access policy sets. For example, a recipient operating under policies inconsistent with the policies of the information provider may use the information in a manner not allowed by the information provider.

TF4FA eliminates the above risk by dynamically creating a Federated Domain wherein participants collaborate in real-time to securely derive access control policy sets and other trust attributes (e.g., technical frameworks). The result is a mutually-acceptable, highest-common-denominator access policy set that is used consistently across domains to ensure the proper level of trust, protection, and use of all shared information.


 

# 2 FEDERATED DOMAIN MODEL (Normative)

The Federated Domain Model is a UML model that describes the capabilities of authorization/security domains participating in information exchange with other domains using a Federated Policy and capable of the highest level of assurance based on an approved trust contract.

This model facilitates trustworthy co-operation between domains by defining a common set of security and privacy policies that applies to all collaborating entities, derived from the relevant domain-specific policies across all those policy domains. Trust services derive those common security and privacy policies as well as other trust framework information in real-time using electronic representation. The results are codified in a computable Trust Contract, which participants to the access control request transaction agree to abide by without exception.

The set of users, data, derived trust and policy, and computable trust contract from individual domains involved in a cross-domain access control transaction results in a new interoperability domain called a Federated Domain. A user can be a person, process, or device.

Broadly speaking, a Federated Domain is a collection of realms that have established a producer-consumer relationship whereby one realm can provide authorized access to a resource it manages to an entity in another realm requesting access. This is accomplished via run-time derivation of trust and access control policies, and the conveyance of access control attributes. Federated authorization is a subset of the broader federation concept that, per [WS-Federation] includes the brokering of identity, attribute, authentication and authorization assertions between realms. A Federated Domain assumes that any necessary identity brokering has been successfully completed prior to the authorization/access processing.

The following diagram shows the logical components required to derived a Trust Contract and Security Policy across two domains (A and B).


 

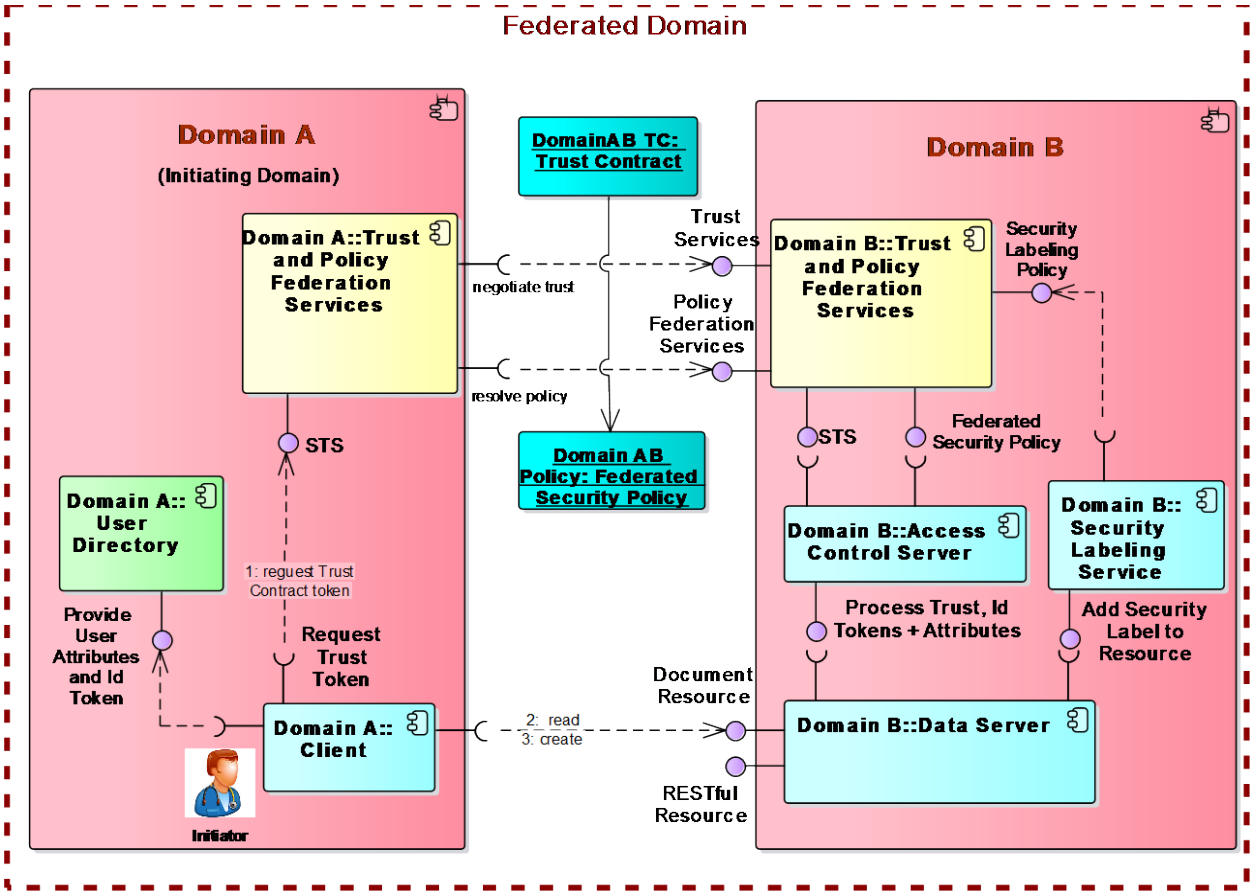


**Figure 3: Federated Domain – Logical Components**

The following diagram illustrates how the cross domain Trust Contract and associated Federated Security Policy are exposed to the each domain by a local domain Trust and Policy Federation Services component.

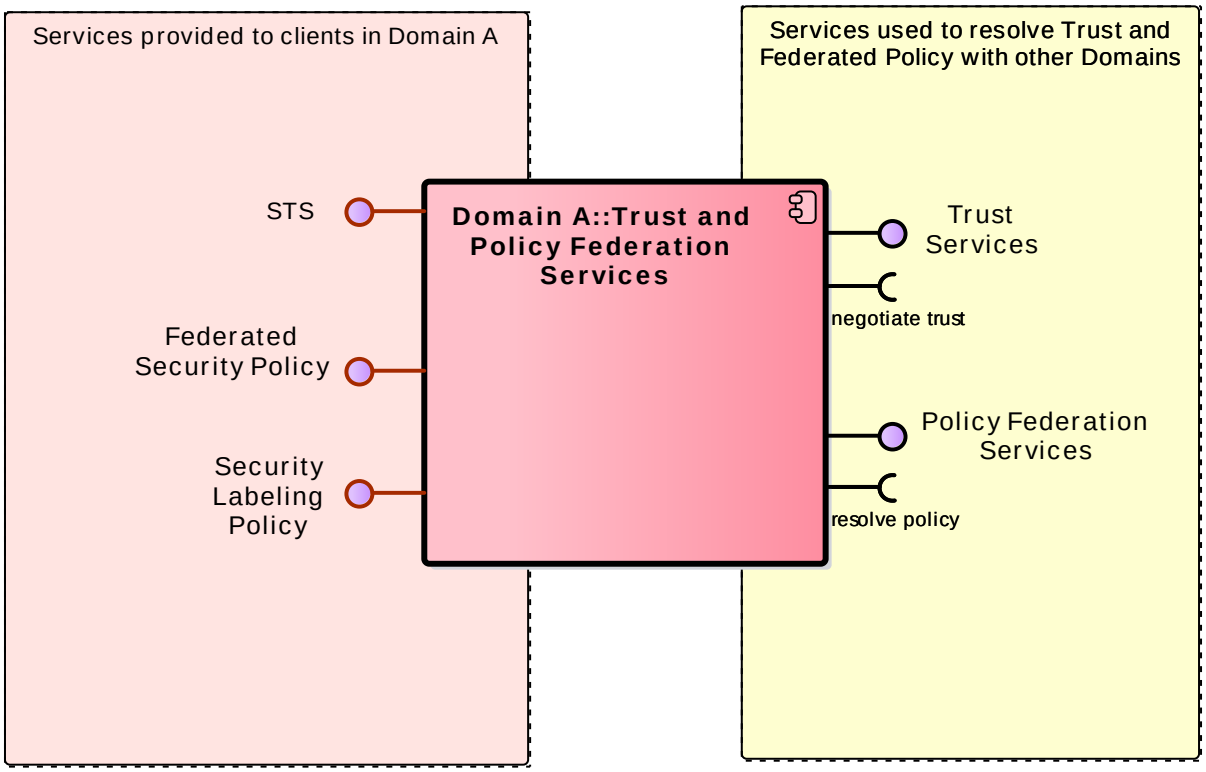


**Figure 4: Federated Domain – Capabilities**

- **Initiator** - An Initiator is an entity (e.g., human user, computer-based entity such as a software application or process, physical device) that attempts to access other entities. [ISO 10181-3]. This class is derived from ISO 10181-3.
- **Domain AB TC** - This object represents the instance of Trust Contract derived by Domains A and B. This Trust Contract is approved/signed off by Domains A and B, the members of the Federated Domain (i.e., Domain AB).
- **Domain AB Policy** - This in an instance of a Federated Security Policy.

## 2.1 Domain A

This is an example Initiating Domain that discovers, and initiates trust and policy derivation with another authorization/security domain (i.e., Domain B).

### 2.1.1 User Directory

It is a component that manages the users across the domain using a standard specification (e.g., IHE Healthcare Provider Directory - US Extension).

**Table 1: User Directory**

| Element | Notes |
|---|---|
| ProvidedInterface Provide User Attributes and Id Token | The User Directory manages the users and their access control attributes. Client application will rely on the directory to authenticate and authorize users. |

### 2.1.2 Client

An application that exchanges information with a Data Server in another domain (i.e.,, Domain B) where a Data Server system provides capabilities to retrieve and add/update information across domains.

### 2.1.3 Trust and Policy Federation Services

This logical component manages the Trust Contract and Federated Security Policy. The initiating domain (Domain A) initiates derivation of Trust Contracts and Federated Security Policies with other domains.

**Table 2: Trust and Policy Federation Services (Domain A)**

| Element | Notes |
|---|---|
| ProvidedInterface STS | A secure trust service (STS) is a software-based identity provider responsible for issuing security tokens as part of a claims-based identity system. In a typical usage scenario, a client requests access to a secure software application, often called a relying party or RP. [WS-TRUST] In this framework, the STS supports tokens or trustmarks required for trust and policy federation across domains including tokens asserting currently certified capabilities. Certified refers to conformance to a well-defined set of requirements specified for that capability. The requirements derive from a recognized, trustmark defining organization.<br>A trustmark attribute is used to specify the certified capability, which can be any service or offering that is certified to provide relying parties trust and confidence in the capability.<br>A trustmark definition is developed and maintained by a Trustmark Defining Organization, which represents the interests of one or more stakeholder communities. A trustmark definition specifies the conformance criteria a Trustmark Recipient must meet, as well as the formal assessment process a Trustmark Provider must perform to assess whether the Trustmark Recipient qualifies for the Trustmark. [GTRI]<br>Trustmarks are backed by rigorous third-party validation, assessment, or auditing. Since the integrity of a trustmark is essential, a trustmark signature must be electronically verifiable to prevent spoofing or modification. [NISTIR 8149] |


 

## 2.2 Domain B

This is an example domain that provides data and responds to requests to derive policy. This domain is also demonstrating the data sharing capabilities exposed by a domain in the Federation Authorization Domain.

### 2.2.1 Trust and Policy Federation Services

Similar to Domain A's Trust and Policy Federation Services, this logical component implements the trust services and policy federation capabilities/services required for trust and policy resolution across domains.

**Table 3: Trust and Policy Federation Services (Domain B)**

| Element | Notes |
|---|---|
| ProvidedInterface Trust Services | The Trust Services are exposed to the initiating domain through a service endpoint (i.e., URL). These services are discoverable by domain to initiate the derivation and agreement on a common Trust Contract. |
| ProvidedInterface Policy Federation Services | This service provides the domain with access to the Federated Security Policy resolved between domain. Domain B exposes Policy Federation Services to an initiating domain (e.g., Domain A). The Policy Federation Services are exposed through this service endpoint (i.e., URL) to an initiating domain. |
| ProvidedInterface Federated Security Policy | This service exposes the access control policies derived part of the Federated Security Policy to other domain systems (e.g., Access Control Server). |
| ProvidedInterface Security Labeling Policy | This service exposes the derived Security Labeling Policy to the domain Security Labeling Service that require these policy and security label definitions. |

### 2.2.2 Data Server

The Data Server conforms to one or more Technical Frameworks asserted during trust derivation (assertTechnicalFramework (ConformanceStatements)). To establish trust between domains, it's important that standard-based interoperability between domains be certified. For instance, the Data Server could be based on technical specifications.

The Data Server uses the Access Control capabilities of its domain to respond to requests initiated from a federated domain (i.e., Domain A). The Data Server uses the request attributes (i.e., user ACI) and ACI computed by its own Security Labeling Service (i.e., Security Labels) to determine whether the user is authorized to execute an operation (e.g., read, created) against a specific data resource.

**Table 4: Data Server**

| Element | Notes |
|---|---|
| ProvidedInterface Document Resource | This is an example document-based data exchange capability (e.g., eHeatlh Exchange based on IHE integration profiles certified by the Sequoia Project). A trusted domain may be conformant and certified by a national certification body. |
| ProvidedInterface RESTful Resource | This is an example data exchange capability based on REST-based resources (e.g., HL7 FHIR). The conformance statements for this type of exchange may reference Data Access Framework (DAF) or Argonaut profiles. |

### 2.2.3 Access Control Server

The Access Control Server evaluates the tokens and attributes submitted by the Client application from Domain A. It uses the STS and the Federated Security Policy to establish and evaluate the policies that apply to specific request.

**Table 5: Access Control Server**

| Element | Notes |
|---|---|
| ProvidedInterface Process Trust, Id Tokens + Attributes | The Access Control Server evaluates the tokens and attributes submitted by a Client application. |

### 2.2.4 Security Labeling Service

This logical component evaluates the domain-specific (e.g., Consent) and Federated Security Policy to label data resources with appropriate security labels and intended recipient information specified by patient consent.

**Table 6: Security Labeling Service**

| Element | Notes |
|---|---|
| Add Security Label to Resource | (add information) |

# 3 INFORMATION MODEL (Normative)

The Policy Information Model is a UML model that describes the policy information model needed to make a proper access request and use decision. The information model elaborates three aspects:

- Trust Contract
- Federated Policy agreed by domains
- Labeled Data Resources with Provenance and Consent-derived metadata

The policy information model is predicated on the establishment of a Security and Privacy Policy Framework being established that ensures an implemented Federated Domain is user-centric. This means the owners of healthcare information maintain control over the sharing and use of their information. Accordingly, the framework should define the rules around access control security and privacy policy, permissible flows of policy, patient consent models, rules for participating domains to bridge differences in policy, and use of agreed upon policies.

The main level focuses on Security Policy and its relationship to other essential high-level classes. The main level fundamentally derives from International Organization for Standardization (ISO) 22600-2. All ISO 22600-2 model elements have been retained and several enhancements incorporated. The enhancements address features (e.g., attribute-based access control) discussed in other standards such as ISO 10181-3 and other models such as the HL7 Domain Analysis Model (DAM), which is incorporated herein by reference.

An information model is an abstract representation of a subject area of interest designed to provide a generic representation of a class of system or capability and to suggest a set of approaches to implementation. This information model is complete enough to enable the development of downstream platform-independent models such as a Reference Information Model-based information, and services models. This information model may also be used to constrain other standards for use in healthcare (e.g., to constrain access control markup standards).

## 3.1 Trust Contract Model

Trust contracts are predicated on the establishment of a legal framework that requires members to agree on a legally binding set of criteria to manage the risk of participating in a contractual trust framework. This includes, but is not limited to, terms for participation and termination, conformance to applicable laws and mandates such as Federal Information Security Management Act (FISMA), HIPAA, and the Privacy Act; permitted uses of information exchanged between members, and waivers/exceptions if any.

In this model, a trust contract makes the business and technical operational rules of a domain legally binding upon its members. Trust contracts are subject to jurisdictional, organizational and subject of care policies that apply equally to all members. Trust contracts can have a time limit, whereupon a new, complete trust contract must be established.

The following diagram identifies the content of the Trust Contract and Federated Policy resolved between two domains:


 

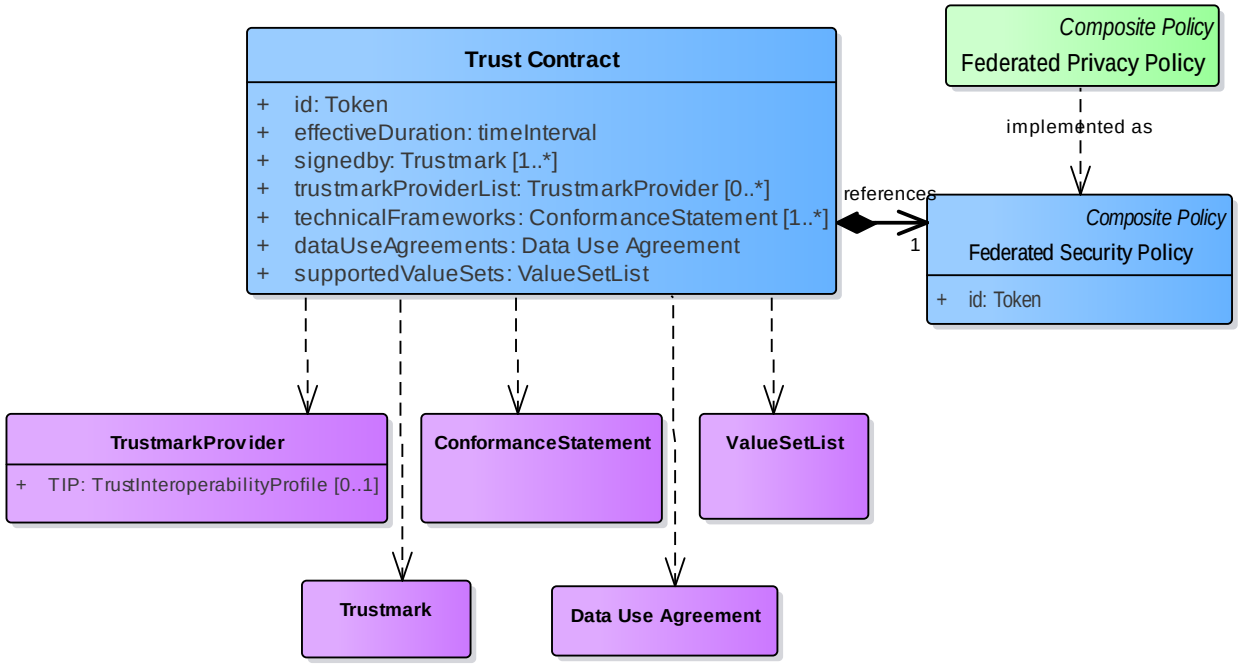


**Figure 5: Trust Contracts and Federated Policy Content**

## 3.2 Trust Contract

The Trust Contract is created by using a set of Trust Services to derive the framework used by two authorization domains.

**Table 7: Trust Contract**

| Attribute | Notes |
|---|---|
| **id** Token<br>Public | Unique id of each Trust Contract. |
| **effectiveDuration** timeInterval<br>Public | The time interval the Trust Contract is if effect. |
| **signedby** Trustmark<br>Public<br>[1..*] | List of stakeholders (e.g., Chief Security Officers) who approved a Trust Contract. |
| **trustmarkProviderList** TrustmarkProvider<br>Public<br>[0..*] | Trustmark Providers used by domains is derived using assertTrustmarkProvider(TrustmarkProviderList) |

| Attribute | Notes |
|---|---|
| **technicalFrameworks** ConformanceStatement<br>Public<br>[1..*] | Technical frameworks used for information exchange, authorization, terminology (i.e., value sets) and data use agreements. The list of Conformance Statement is derived using assertTechnicalFramework(ConformanceStatements) service. |
| **dataUseAgreements** Data Use Agreement<br>Public | Data Use Agreements supported by the federated domain. This list is derived using the assertDataUseAgreements(DataUseAgreementList) service. |
| **supportedValueSets** ValueSetList<br>Public | Value sets supported by the domains - including value sets used to evaluate the Federated Security Policy resolved between domains using assertValueSets(ValueSetList). |

### 3.3 TrustmarkProvider

This is a list of supported Trustmark Providers (TPs) [GTRI]. TPs are analogous to PKI Certificate Authorities. [GTRI - Parallels between Trustmarks and PKI]

**Table 8: TrustmarkProvider**

| Attribute | Notes |
|---|---|
| **TIP** TrustInteroperabilityProfile<br>Public<br>[0..1] | A Trustmark Interoperability Profile is essentially a formal statement that lists the trustmarks that one entity must have in order to be trusted by, and interoperable with, another entity. It is analogous to a List of Trusted Certificated Authorities [GTRI - Parallels between Trustmarks and PKI]. |

### 3.4 ConformanceStatement

Conformance Statements describes integration profiles, actors, implementation guides, profiles, templates, and terminology constraints.

These statements may include endpoint URLs and other information required to exchange information as well as token asserting currently certified capabilities. Certified refers to conformance to a well-defined set of requirements specified for that capability. (see STS).

**Example**: A formal representations of conformance statements may use FHIR CapabilityStatement resource to express the capabilities of a Domain to share data with another domain using FHIR RESTful services.

### 3.5 ValueSetList

The list of Value Sets that organizes the standard-based terminology required to represent authorization and other elements of the Federated Policy and Security Label Definitions.


 

### 3.6 Data Use Agreement

The Trust Contract specifies one or more Data Use Agreements (e.g., Center for Medicaid and Medicare Services DUA forms). If the domains use eHealth Exchange/Sequoia Project, these domains will use the Data Use and Reciprocal Support Agreement (DURSA).

### 3.7 Trustmark

GTRI defines **trustmark** as "a statement of conformance to a well-scoped set of identity trust and/or interoperability requirements." [GTRI] It is s analogous to a Public Key Infrastructure (PKI) certificate in that a Trustmark (Certificate) represents a specific set of facts asserted to a Trustmark Relying Party (Certificate Relying Party, or Audience) about a Trustmark Recipient (Subscriber).

The roles, responsibilities, and terms of use for a Trustmark (Certificate) are described in a Trustmark Policy (Certificate Policy).

The scope and terms of the legal agreement between the Trustmark Provider (Certificate Authority) and the Trustmark Recipient (Subscriber) are delineated in a Trustmark Agreement (Subscriber Agreement). [GTRI - Parallels between Trustmarks and PKI]


 

# 4 FEDERATED POLICY MODEL (Normative)

Federated Policy is the result of an automated resolution process using a set of “Policy Federation Services“ that resolve the security policy differences across domain to arrive at the highest level of services and assurance possible.

The following diagram shows the structure of a security policy derived by domains participating in a Federated Domain:

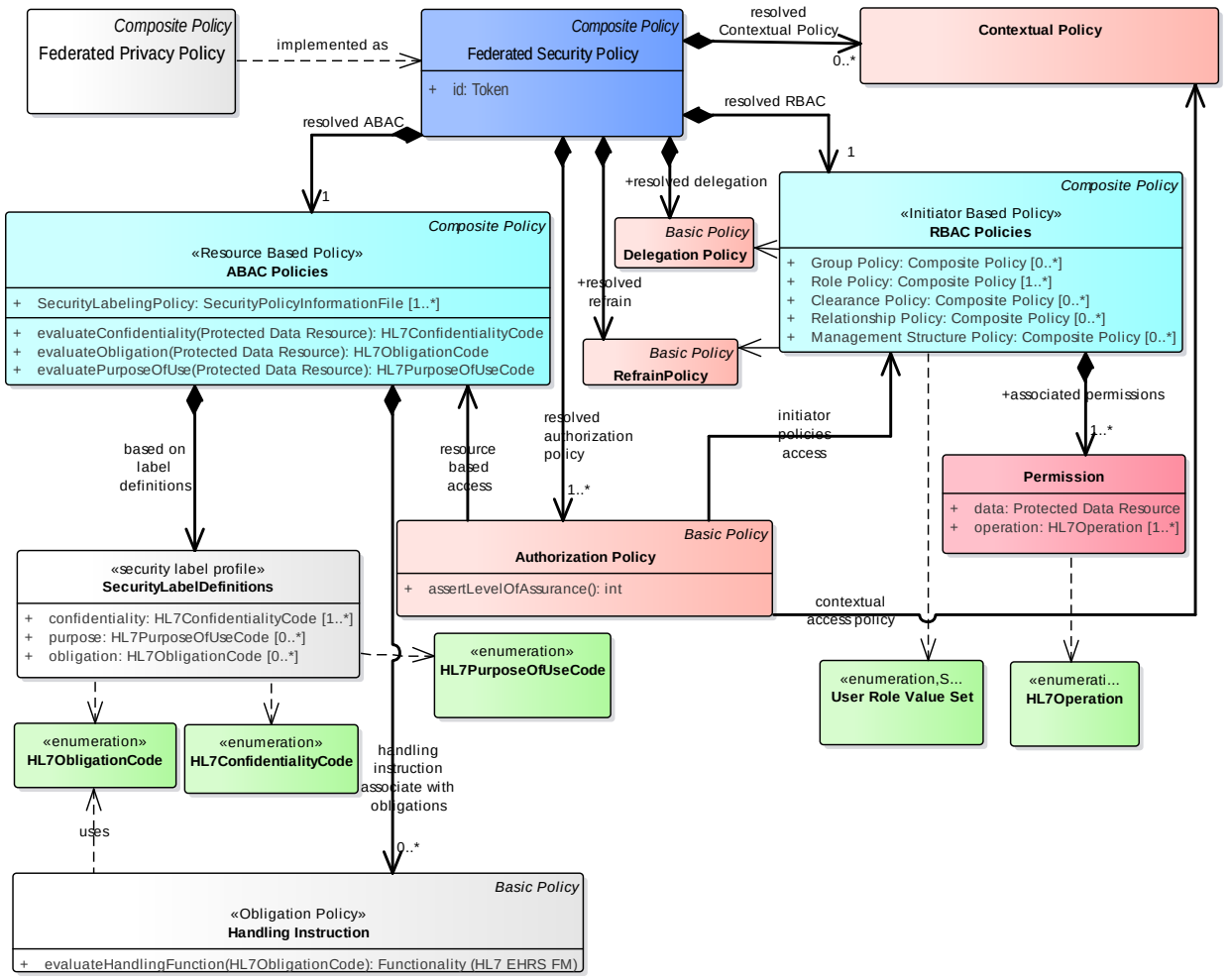


**Figure 6: Federated Policy**

## 4.1 Federated Security Policy

A policy is a “set of legal, political, organizational, functional and technical obligations for communication and cooperation.” Policy governs the behavior of a system. [ISO 22600-2]

Policy encompasses jurisdictional, organizational, and Subject of Care (patient) policies. Organization and jurisdictional policies are instantiated as Basic Policy in both the security policy and privacy policy contexts. Basic Policy is discussed later in this document. It should also be noted that privacy policy is controlled by the Subject of Care.

The Federated Security Policy resolved by the domains as the combination of authorization and other policies supported by the combined/federated domains is expressed as a combination of resolved policies:

- Authorization Policy that addresses the minimum Level of Assurance allowed by combined domain.
- Initiator-Based Access Control Policy (i.e., Role-Based Access Control)
- Information Resource Access Control Policy (i.e., Attribute-Based Access Control)

These policies use a set of derived SecurityLabelDefinitions based on

- Contextual Policy
- Delegation Policy
- RefrainPolicy

**Table 9: Federated Security Policy**

| Attribute | Notes |
|---|---|
| **id** Token<br>Public | Identity token of the resolved security policy agreed by federated security domains. It consists of a set of resolved policy sets. |

### 4.2 Federated Privacy Policy

This class describes cross-domain Privacy Policy that is realized and implemented by the Federated Security Policy resolved by the domains.

A Privacy Policy describes a set rules that govern the behavior of systems and users in order to accomplish an overall objective (e.g., protect patients from perceived social stigma associated with a specific disorder). It contains a set of rules that are intended to be enforced by security systems and are used as the basis for Subject of Care privacy consent directives. The structure of a Privacy Policy is specified in the HL7 DAM.

This class derives from ISO 22600-2 and HL7 DAM.

### 4.3 Authorization Policy

Authorization policies are essentially security policies related to access-control and specify what activities a subject is permitted or forbidden to do, to a set of target objects. They are designed to protect target objects so are interpreted by access control agents or the run-time systems at the target system. [PONDER]

Authorization Policy is a specialization of a Basic Policy.

This class derives from ISO 22600-2 and HL7 DAM.

**Table 10: Authorization Policy**

| Services | Notes | Parameters |
|---|---|---|
| **assertLevelOfAssurance ( )** int | The Electronic Authentication should use a consistent Level of Assurance across a Domain and it must be agreed to among the domains in accordance to the NIST Electronic Authentication Guideline [NIST SP 800-63-3]. | |

## 4.4 RBAC Policies

This class specifies a set of Role-based Access Control (RBAC) policies specified by ISO 10181-3 as "Initiator-based access control Policies". Two categories of security policy, rule-based and identity-based, are identified in International Telegraph and Telephone Consultative Committee (CCITT) Rec. X.800 | ISO 7498-2. [ISO 10181-3]

Initiator-based access control policies are based on rules specific to an individual initiator, a group of initiators, entities acting on behalf of initiators, or originators acting in a specific role. Access control policies stated in terms of groups of initiators or in terms of initiators acting in specific roles are types of initiator-based policies. [ISO 10181-3]

**Table 11: RBAC Policies**

| Attribute | Notes |
|---|---|
| **Group Policy** Composite Policy<br>Public<br>[0..*] | Group Policy defines a scope for related policies to which a set of constraints can apply. [ISO/TS 22600-2]<br>A group is a set of initiators whose members are considered equivalent when a particular access control policy is enforced. Groups allow access to particular targets by a set of initiators without the necessity of including the identity of individual initiators in a target's ACI, and without explicitly allocating the same ACI to each initiator. The composition of a group is determined by a management action; the ability to create or modify groups must be subject to access control. Audit of access requests by the group without distinguishing the members may or may not be required. [ISO 10181-3]<br>If one considers an initiator identity as initiator-bound ACI, and a set of (initiator identity, operation type) pairs as target-bound ACI, under an appropriate access control policy, one obtains what is essentially an access control list (ACL) scheme [ISO 10181-3]. Accordingly, the Group Policy class equates to the ISO 10181-3 ACL scheme.<br>This policy definition derives from ISO/TS 22600-2, HL7 DAM, and ISO 10181-3. |
| **Role Policy** Composite Policy<br>Public<br>[1..*] | Role Policy is used to specify the attributes identifying the user of a system used to access Protected Information. A role is a specialization of Composite Policy that defines a group of policies (authorization, obligation, delegation and refrain policies). [HL7 DAM]<br>ISO-22600 more specifically defines a role as a "set of competencies and/or performances which is associated with a task." |

| Attribute | Notes |
|---|---|
| | If one considers a set of (target identity, operation type) pairs as initiator-bound ACI, and target identities as target-bound ACI, under an appropriate access control policy, one obtains what is essentially a capability scheme [ISO 10181-3]. Accordingly, the Role Policy class equates to the ISO 10181-3 capability scheme.<br>**Functional roles** reflect functional aspects of relationships between entities. Functional roles are bound to the realization/performance of acts, where actions might be concatenated to an activity or even to a process. [ISO/TS 22600-2]<br>Functional Roles can be grouped according to their authorization to access Protected Information and perform various operations on healthcare information. For example, a healthcare provider in Organization A is authorized to access Protected Information from Organization B (when Organization A and B have entered into a trusted relationship) if that provider is associated with the Functional Group whose permissions grant access per that Functional Role. In summary, the functional role defines the access control decision. A functional role is bound to a policy. [HL7 DAM]<br>**Structural roles** reflect the structural aspects of relationships between entities. Structural roles describe prerequisites, feasibilities, or competencies for acts. [ISO/TS 22600-2]<br>Note that this role is called a "Session Role" in American National Standards Institute (ANSI) / InterNational Committee for Information Technology Standards (INCITS). [FHIM]<br>Structural Role is used to illustrate the type of roles that may be used in a privacy policy or Role Based Access Control (RBAC) permission. Structural codes are currently provided by ASTM E1986-09. [HL7 DAM]<br>Functional and Structure Roles are derived from ISO/TS 22600-2 and HL7 DAM. |
| **Clearance Policy**<br>Composite Policy<br>Public<br>[0..*] | If one considers what are commonly called "clearance" and "classification" as initiator-bound ACI and target-bound ACI, respectively, under an appropriate access control policy, one obtains what is essentially a label-based scheme. [ISO 10181-3] In this case, there is a policy to bind clearance to Initiators (e.g., persons who work with blood need HIV clearance) and policy for Resources (e.g., Human Immunodeficiency Virus information is considered "sensitive" and has code "HIV"). Accordingly, Clearance Policy falls under the Initiator Based Policy class, the Clearance Policy class equates to the ISO 10181-3 label-based scheme.<br>Initiator-bound clearance ACI can be compared with security labels of Resources. Examples of clearance ACI are "Top Secret," "Secret," and "Confidential." [HL7 PASS SLS]<br>This policy definition derives from ISO 10181-3 |
| **Relationship Policy**<br>Composite Policy<br>Public<br>[0..*] | Relationship Policy defines a group of policies pertaining to the interactions between a set of roles. [ISO/TS 22600-2]<br>This policy definition derives from ISO/TS 22600-2. |

## 4.5 ABAC Policies

This class specifies "Information Resource Policies" that support Attribute-based access control (ABAC). ABAC defines an access control paradigm whereby access rights are granted to users through the use of policies which combine attributes together.

**Table 12: ABAC Policies**

| Attribute | Notes | |
|---|---|---|
| **SecurityLabelingPolicy**<br>SecurityPolicyInformationFile<br>Public<br>[1..*] | The most important element of ABAC is the Security Labeling Policy - implemented as a Security Policy Information File (SPIF). | |
| **Services** | **Notes** | **Parameters** |
| **evaluateConfidentiality()**<br>HL7ConfidentialityCode | None | **Protected Data Resource ]**<br>**dataResource** |
| **evaluateObligation()**<br>HL7ObligationCode | None | **Protected Data Resource ]**<br>**dataResource** |
| **evaluatePurposeOfUse()**<br>HL7PurposeOfUseCode | None | **Protected Data Resource ]**<br>**dataResource** |

## 4.6 SecurityLabelDefinitions

This class represents a profile of the Security Label Specification consistent with Meaningful Use 2015 optional certification criteria for security metadata. The HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 specifies a simplified set of labels.

**Table 13: SecurityLabelDefinitions**

| Attribute | Notes |
|---|---|
| **confidentiality**<br>HL7ConfidentialityCode<br>Public<br>[1..*] | This security label field is a mandatory security label field that specifies the confidentiality level of a data resource.<br>Security label metadata that specifies the labeled resource's level of confidentiality. The level of confidentiality specifies the degree of protection against access the data or information requires, together with a designation of that degree of protection. [HL7 PASS SLS]<br>Level of confidentiality values are set in accordance with [HL7 HCS Vocab]. Examples of values are "**V**" for "Very Restricted", "**R**" for "Restricted", and "**N**" for "Normal"<br>In general, classification is the confidential protection of data elements by segmentation into restricted and specifically controlled categories set by policies, professional practice, and laws, legislation, and regulations. [HL7 |

| Attribute | Notes |
|---|---|
| | HCS, adapted from ASTM E1986]<br>This class derives from HL7 HCS, HL7 PASS SLS, and HL7 DAM. |
| **purpose**<br>HL7PurposeOfUseCode<br>Public<br>[0..*] | Security label metadata that specifies the permissions about how a resource may be used to which a sender or a receiver must comply. [HL7 PASS SLS]<br>Purpose of Use (POU) values specify permitted uses. The values are in accordance with [HL7 HCS Vocab]. |
| **obligation**<br>HL7ObligationCode<br>Public<br>[0..*] | Security label metadata conveys dissemination controls and information handling instructions such as obligations and refrain policies to which a resource custodian or receiver must comply. This type of handling caveat must be assigned to a clinical fact if required by jurisdictional or organizational policy, which may be triggered by a Subject of Care consent directive. Example handling instructions are: do not disclose, restrictions on use, and policy marks. [HL7 HCS]<br>This label is conditional of a successful derivation of Handling Instruction Policies across domains. |

### 4.7 Contextual Policy

A Contextual Policy defines control of access according to its context (see ACI for additional details on Context Information). Contextual Policy can modify Initiator-based Policy or Information Resource Policy. Context rules may define the entire policy in effect. Contextual information is information about or derived from the context in which an access request is made (e.g., time of attempted access, location of the accessor, route of access). [ISO 10181-3]

Rules concerning contextual information are most often used in conjunction with other access control schemes (e.g., label-based scheme, capability scheme, ACL scheme), but they may be used alone to create a context-based access control scheme. [ISO 10181-3]

### 4.8 Refrain Policy

Refrain policies specify what a subject must refrain from doing and are similar to negative Authorization Policies but are interpreted by the subject. [PONDER]

A Refrain Policy is used to constrain an existing policy by indicating that a specific action is prohibited based on specific access control attributes (e.g., purpose of use, information type, user role). For example, a Refrain Policy instance may be used to represent a privacy consent directive that sets specific “limitations” on a default organizational policy regarding substance abuse data (e.g., [42 CFR Part 2]). [HL7DAM]

Refrain Policy is a specialization of the “Basic Policy” class. It does not have any additional attributes but implies different behavior. [HL7 DAM]

### 4.9 Basic Policy

This is the base class for a variety of policy types. It extends the abstract Federated Policy class and provides additional attributes. This class may be used to instantiate specific policies. ISO-22600-2 specifies a Security Policy as a “plan or course of action adopted for providing computer security.”

A Basic Policy encompasses jurisdictional and organizational policies via five types of security and privacy policies: Authorization Policy, Refrain Policy, Obligation Policy, Delegation Policy, and Privacy Policy.

### 4.10 Composite Policy

Composite Policy is used to group a set of related policy specifications within a syntactic scope with shared declarations in order to simplify the policy specification task for large distributed systems. Constraints can be specified to limit the applicability of policies based on time or values of the attributes of the objects to which the policy refers. [PONDER].

A Composite Policy is the integration point between Security and Privacy perspectives. It contains a set of basic policies that work together to enforce a privacy policy, organizational standard operating procedure, or a privacy consent directive. Its basic characteristic is that it contains other policies. An instance of a Composite Policy may include several Authorization, Delegation, Refrain, Obligation, or Privacy policies. A Composite Policy is specialization of the abstract Policy class and inherits all its attributes and associations. In addition to the attributes it inherits from its base class ("Policy"), this type of class contains additional associations and attributes. [HL7 DAM]

### 4.11 Handling Instruction

Security label metadata conveys dissemination controls and information handling instructions such as obligations and refrain policies to which a resource custodian or receiver must comply. This type of handling caveat must be assigned to a clinical fact if required by jurisdictional or organizational policy, which may be triggered by a Subject of Care consent directive. Example handling instructions are: do not disclose, restrictions on use, and policy marks. [HL7 HCS]

Obligation policies specify what activities a subject must do to a set of target objects and define the duties of the policy subject. Obligation policies are triggered by events and are normally interpreted by a manager agent at the subject. [PONDER]

An obligation is an operation specified in a rule, policy, or policy set that should be performed by the Policy Enforcement Point in conjunction with the enforcement of an authorization decision [XACML]. In short, obligations are actions to be performed [ISO 22600-2].

An Obligation Policy may be used to specify additional privacy preferences specified by a Subject of Care. An Obligation Policy may be specified in addition to a Refrain Policy to fully describe a client's access control preferences. In some cases, an Obligation Policy may be used to indicate that the receiver of an information object may not be allowed to re-disclose or persist that information object indefinitely. [HL7 DAM]


 

**Table 14: Handling Instruction**

| Services | Notes | Parameters |
|---|---|---|
| **evaluateHandlingFunction()** Functionality (HL7 EHRS FM) | The handling instructions are associated with specific systems behaviors that could be expressed "functionality" specified in the HL7 EHR Functional Model | **HL7ObligationCode** ]<br>**obligationLabel** |

## 4.12 Permission

This class corresponds to an RBAC permission. It specifies an information object and action/operation allowed on that object. A permission contains one operation and precisely one information reference. [HL7 DAM]

**Table 15: Permission**

| Attribute | Notes |
|---|---|
| **data** Protected Data Resource<br>Public | None |
| **operation**<br>HL7Operation<br>Public<br>[1..*] | None |

## 4.13 Delegation Policy

Delegation is the "conveyance of privilege from one entity that holds such privilege, to another entity." [ISO 22600-2]

Delegation Policies specify which actions subjects are allowed to delegate to others. A delegation policy thus specifies an authorization to delegate. [PONDER]

In other words, Delegation Policy defines what authorizations can be delegated to whom. Delegation may be to a specific individual or organization.

## 4.14 User Role Value Set

The User Role value set is defined by the NHIN Specifications Factory to the restricted set of SNOMED CT codes listed in Table 2-155 Author Role Value Set Definition.

OID: 2.16.840.1.113883.3.18.6.1.15

Source: National Health Information Network (NHIN)

# 5 LABELING AND PROVENANCE (Normative)

This section of the information model illustrates how each domain in the Federated Domain is able to label data elements based on derived policies (i.e., Security Labeling Policy and Security Label Definition) and patient Consent.

Data Servers use Security Labeling Services to evaluate domain and Federated policies along with patient-centric Consent policies to compute the metadata associated with Data Resource, specifically those Protected Data Resources that contain protected clinical facts (e.g., findings, observations, medications) that are encoded using value sets and coding systems identified in the trust contract between domains.

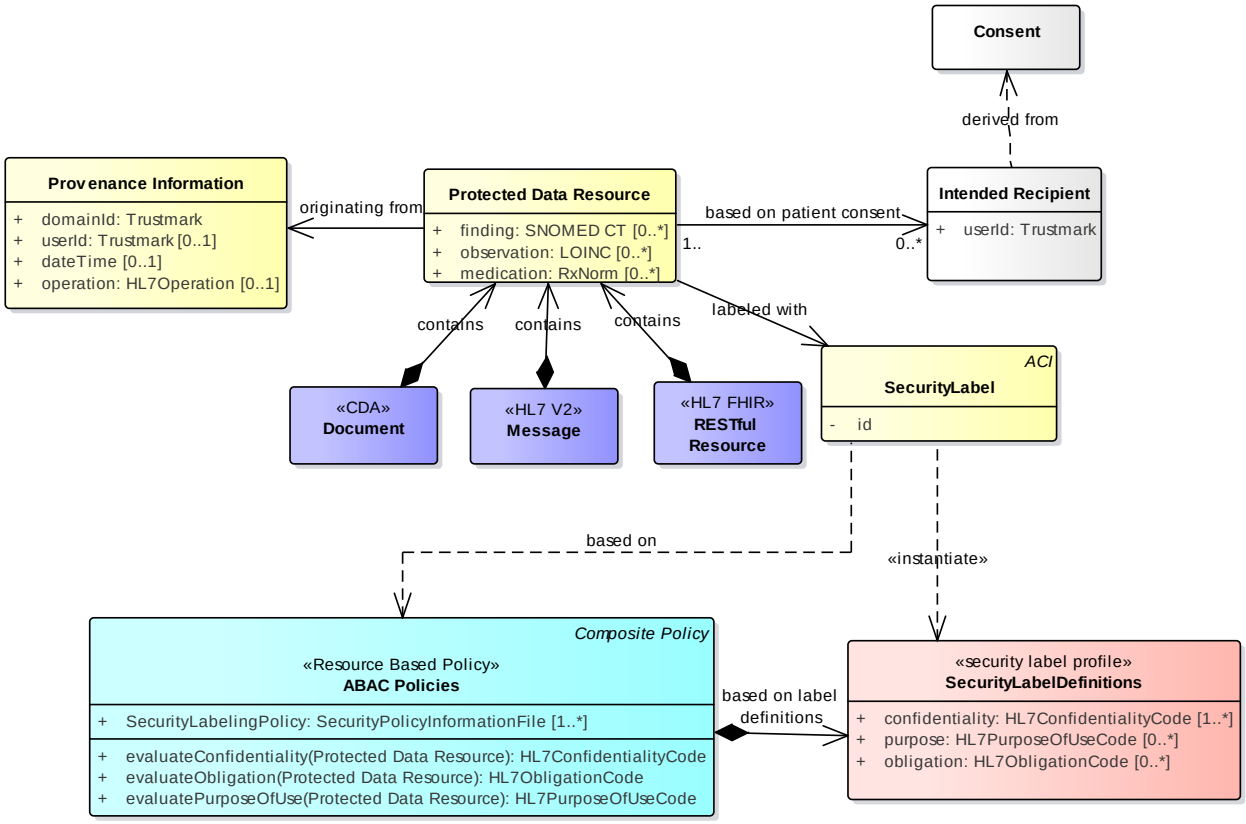


**Figure 7: Protected Data Resources and Metadata**

## 5.1 Protected Data Resource

A Resource (sometimes referred to as data, target, system, or information) is an entity to which access may be attempted. [ISO 10181-3].

Protected Data Resources are labeled with Security Labels based on the resolved Security Label Definition and Security Labeling Policy.

Protected Data Resources may be exchanged using a variety of paradigms: standard-based documents (e.g., CDA Document), messages (e.g., HL7 Version 2 Message) or a REST-based resource (e.g., HL7 FHIR Resource). Each paradigm provides a specific implementation approach for security labeling or provenance. Some of the information may need to be persisted by Data Servers as additional metadata.

**Table 16: Protected Data Resource**

| Attribute | Notes |
|---|---|
| **finding** SNOMED CT<br>Public<br>[0..*] | A Data Resource may contain zero or more clinical finding coded using SNOMED CT.<br>SNOMED CT is used for Meaningful Use certified EHR systems to encode clinical findings (e.g., conditions, symptoms, disorders, observed findings). The federated domain may specify classification policies that identify specific finding as "protected". |
| **observation** LOINC<br>Public<br>[0..*] | A Data Resource may contain observations coded using LOINC. |
| **medication** RxNorm<br>Public<br>[0..*] | A Data Resource may contain medication codes typically encoded using RxNorm by Meaningful Use certified EHR Systems. |

## 5.2 Intended Recipient

The patient's consent may specify one or more providers who are authorized to read/retrieve a specific Protected Data Resource contained in a document, messages, or REST resource.

**Table 17: Intended Recipient**

| Attribute | Notes |
|---|---|
| **userId** Trustmark<br>Public | None |

## 5.3 ACI

Access control information (ACI) is any information used for access control purposes, including contextual information. [ISO 10181-3]

ACI can be either information about a single entity or information about a relationship among entities. For example, ACI allocated to an initiator may be purely about that initiator, or it may be about relationships between that initiator and particular targets, or about relationships between that initiator and possible contexts. [ISO 10181-3]

Access Control Decision Information (ACDI) is a subset of ACI. Security Labels are an example of ACI.

### 5.3.1 Initiator-bound ACI

Examples of Initiator-bound ACI are the access control identity of an individual and roles that may be taken.


 

### 5.3.2 Access Request-bound ACI

An access request encompasses the operations and operands that form part of an attempted access. Examples of Access Request-bound ACI are allowed class of operation (e.g., read, write) and data type of the operation. [ISO 10181-3]

### 5.3.3 Resource-bound ACI

Examples of Resource-bound ACI are target access control identities and sensitivity markings. [ISO 10181-3]

### 5.3.4 Operand-bound ACI

An operand is part of the access request that pertains to the object of the operation. Examples of Operand-bound ACI are the sensitivity markings and integrity markings of the Resource.

### 5.3.5 Retained ADI

Retained Access Control Decision Information (ADI) is ADI that has been retained from earlier access control decisions for use in future access control decisions. ADI is that portion (possibly all) of the ACI made available when making a particular access control decision. [ISO 10181-3]

### 5.3.6 Contextual Information

Contextual information is information about or derived from the context in which an access request is made. Examples of Context-based ACI are time periods, geographic location, purpose of use, and Break Glass instances where the circumstances of a patient needing unanticipated emergency care prompts a provider to override current privileges to access patient information. Note this is in contrast to a provider with clearance for Emergency Treatment purpose of use or access granted non-privileged providers in extraordinary circumstances such as a disaster. [ISO 10181-3]

## 5.4 SecurityLabel

Security Labels are resource-bound ACI that control disclosure of Protected Information. Resource-bound ACI called security labels that control disclosure of Protected Information that is a classification that specifies the degree of protection against access the data or information requires, together with a designation of that degree of protection. [HL7 PASS SLS].

A Security Label instantiates the Security Label Definition and it a specialization of ACI.

**Table 18: Security Label**

| Attribute | Notes |
|---|---|
| **id**<br>Private | None |

# 6 TRUST SERVICES MODEL (Normative)

The Trust Services Model is a UML model (using component definitions and interfaces) that describes the services that derive trust and policy at run-time between domains participating in a cross-domain access request transaction

It also describes the steps required to derive a Trust Contract and the relevant Federated Security Policy.


 

The first priority is deriving the Trust Contract:

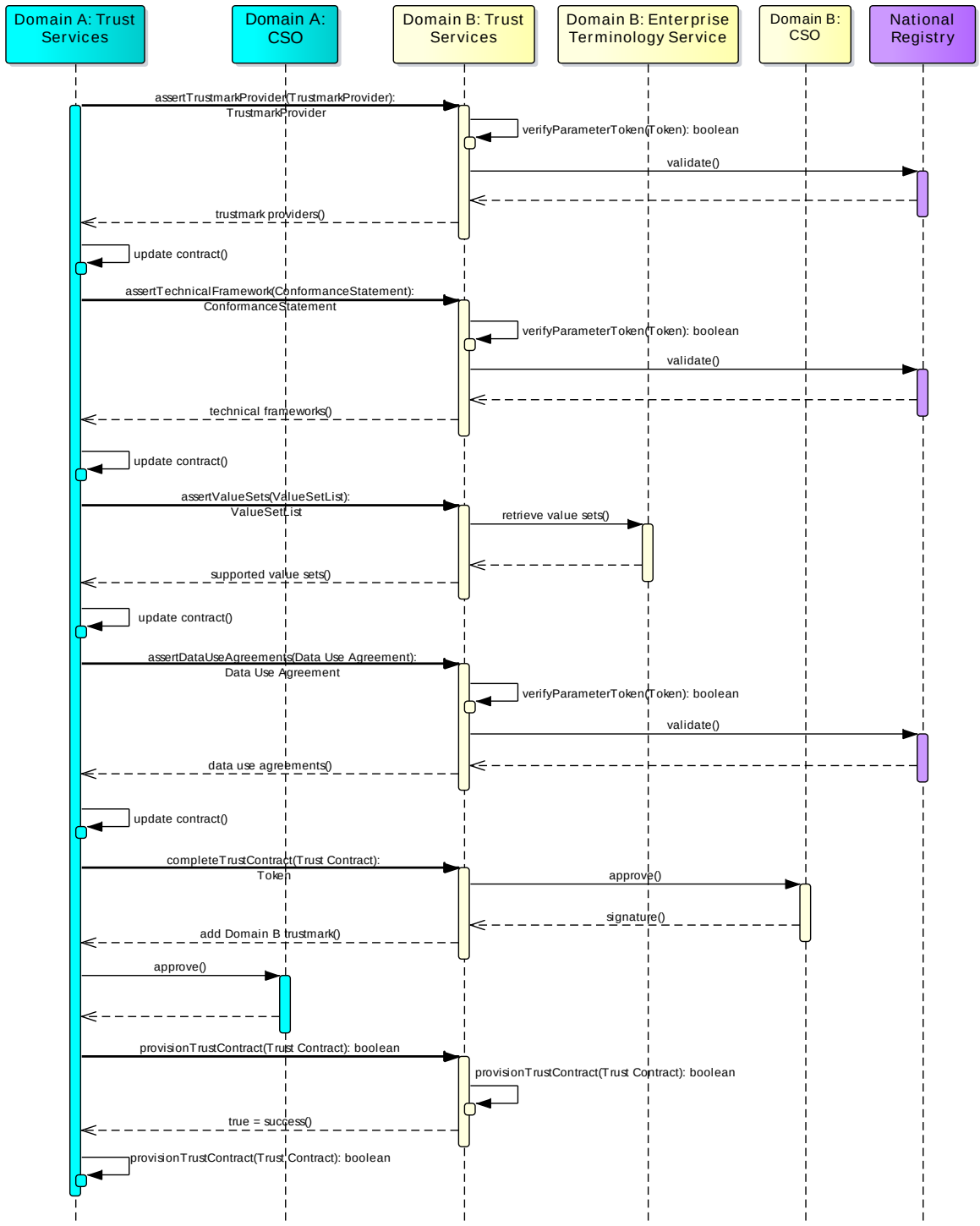


**Figure 8: Resolving Trust Contracts**


 

The following diagram shows how a set of policy resolution services are orchestrated to create a cohesive, federated policy that can be used across a federated domain (i.e., Domain AB Federated Policy consisting of resolved Domains A and B security policies):

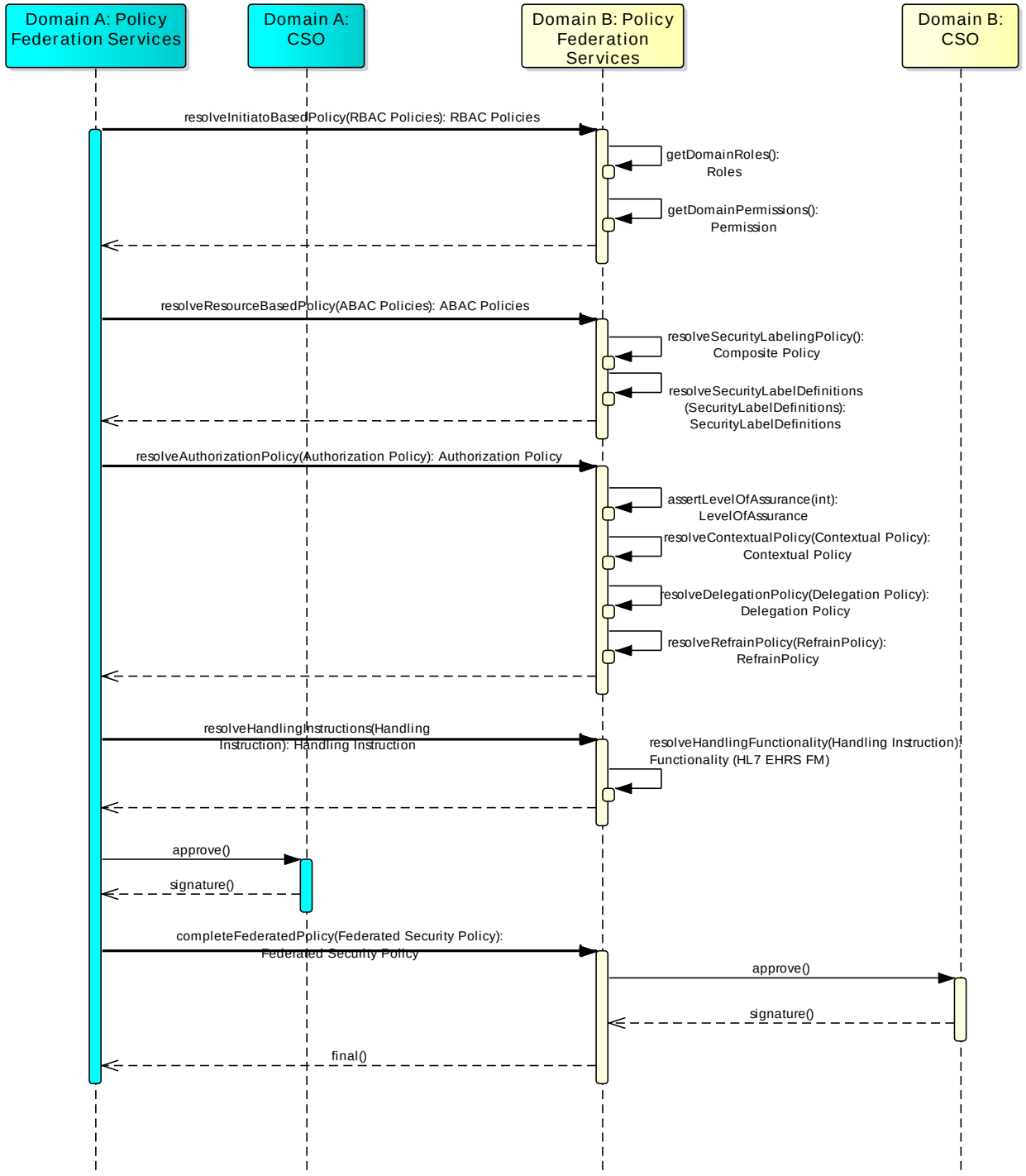


**Figure 9: Resolving Federated Policy**


 

The following are Trust and Policy Federation Services needed to derive trust and policies.

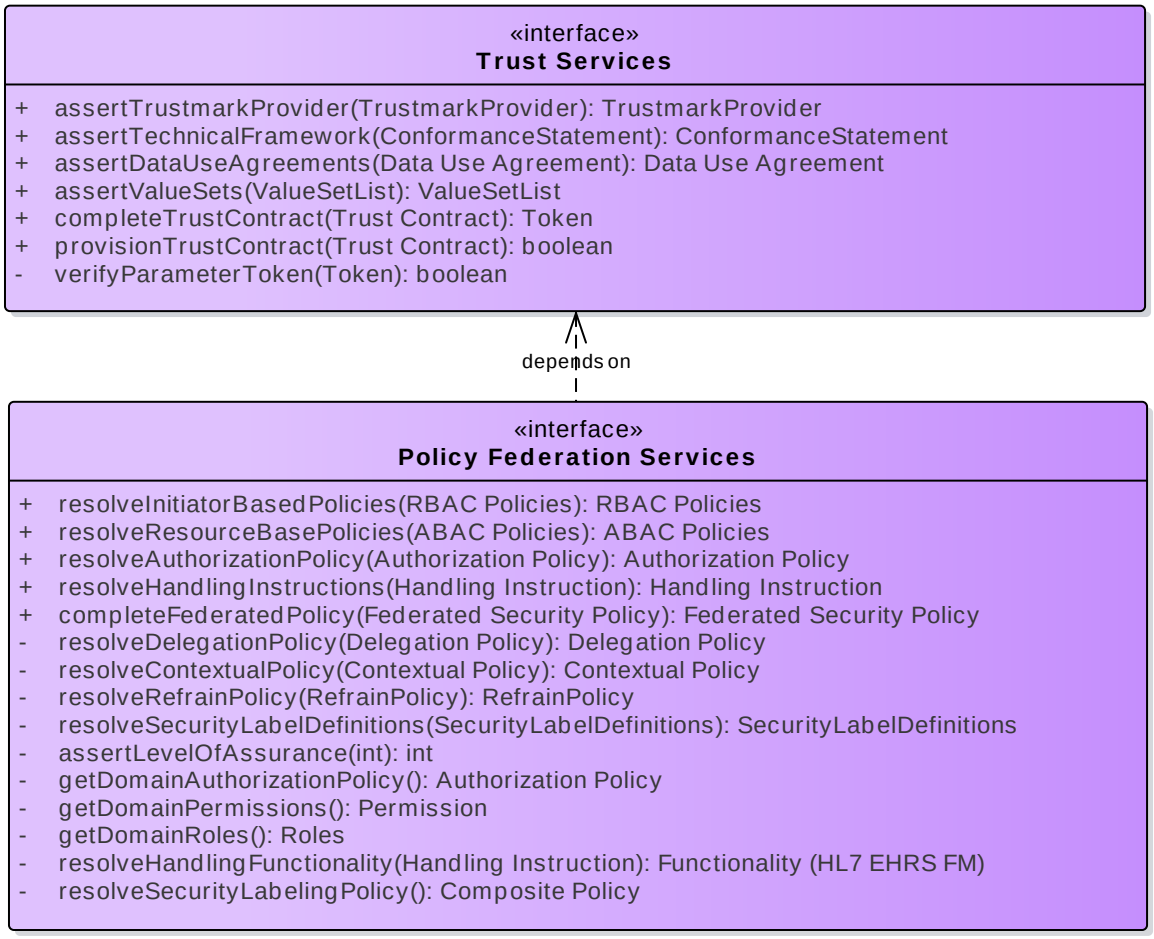


**Figure 10: Trust and Federation Policy Services**

## 6.1 Trust Services

The following are logical trust services provided by the Trust and Policy Federation Services component to other domains. These services are intended to specify several assertions that may be used to establish a federated authorization/security domain.

**Table 19: Trust Services**

| Services | Notes | Parameters |
|---|---|---|
| **assertTrustmarkProvider()** TrustmarkProvider | The initiating domain uses this capability to specify its supported Trustmark Providers. By default, the domains will rely on the Trustmark Interoperability Profile (TIP).<br>The responding domain specifies its supported Trustmark Providers. | **TrustmarkProvider ]**<br>**trustmarkProvider** |

| Services | Notes | Parameters |
|---|---|---|
| **assertTechnicalFramework()** ConformanceStatement | The initiating domain specifies the technical frameworks it supports as a list of Conformance Statements. These technical frameworks typically include authorization specifications (e.g., the NHIN Authorization Framework required by the eHealth Exchange/Sequoia project) .<br>If the domains do not converge on a common set of technical frameworks, the Trust Contract cannot be completed. | **ConformanceStatement ] conformance** |
| **assertDataUseAgreements()** Data Use Agreement | The initiating domain may specify one or more Data Use Agreements that it supports. These may be associated with one or more Technical Frameworks asserted by the domain. The responding domain will return its own set of DUAs. If the domains do not converge on a common set of DUAs, the Trust Contract may not be completed. | **Data Use Agreement ] clientList** |
| **assertValueSets()** ValueSetList | The initiating domain specifies the value sets supported by its Enterprise Terminology Service (or Value Set Service) in order to support federated authorizations, security labeling, and interoperability. If the two domains do not converge on a common set of Value Sets, the Trust Contract may not be completed. | **ValueSetList ] valueSetList** |
| **completeTrustContract()** Token | The final step requires that the Trust Contract is signed by the relevant stakeholders (e.g., domain CSO). | **Trust Contract ] file** |
| **provisionTrustContract()** boolean | The completion of policy resolution is formalized in a **policy decision** by Domain participants to accept the rules for participation in the Trust Framework. The Access Control Service (ACS) for each domain signs and forwards a copy of the derived **trust bundle to each participating Trust Framework member**. This signed **trust bundle** constitutes the derived run-time Trust Contract. | **Trust Contract ] contract** |
| **verifyParameterToken()** boolean | This capability is invoked by a domain responding (e.g., Domain B) to a request to assert a specific aspect of a Trust Contract.<br>This capability is used to establish that the information provided by the initiating | **Token ] token** |

| Services | Notes | Parameters |
|---|---|---|
| | domain is correct and trustworthy based on other sources of information (e.g., security tokens). This capability may require the use of external services (e.g., a National Registry) to perform the verification or based on trustmarks supplied by the initiating domain. | |

## 6.2 Policy Federation Services

The policy resolution services are evaluated to create a Federated Security Policy.

**Table 20: Policy Federation Services**

| Services | Notes | Parameters |
|---|---|---|
| **resolveInitiatorBasedPolicies()** RBAC Policies | This service resolves **Initiator-Based Access Control Policies** (i.e., RBAC Policies) between the two domains. The initiating domain (e.g., Domain A) passes its own RBAC Policies to the other domain (e.g., Domain B) to be resolved into a cohesive Federated RBAC policy. The resolution process reconciles the initiating domain's policy with the responding domain's policy including its domain-specific user roles and permissions. | **RBAC Policies** ]<br>**domainPolicy** |
| **resolveResourceBasePolicies()** ABAC Policies | This service resolves Information Resource Access Control Policies (i.e., ABAC Policies) between the two domains. The initiating domain (e.g., Domain A) passes its own ABAC Policies to the other domain (e.g., Domain B) to be resolved into a cohesive Federated ABAC policy.<br>The domains resolve not only their Security Labeling Policies but also the Security Label Definitions supported. | **ABAC Policies** ]<br>**domainPolicy** |
| **resolveAuthorizationPolicy()** Authorization Policy | This service resolves the Authorization Policy supplied by the initiating domain (i.e., Domain A) against the policies supported by the responding domain (i.e., Domain B) | **Authorization Policy** ]<br>**domainPolicy** |

| Services | Notes | Parameters |
|---|---|---|
| | including:<br>• asserting a common level of assurance<br>• resolve contextual policy associated with the<br>• resolved Initiator-Based and Information Resource Access Control Policies.<br>Optionally, the authorization policy resolution may include:<br>• delegation policy resolution<br>• refrain policy resolution<br>if the domain uses these policies for authorizing user access to data resources across domains. | |
| **resolveHandlingInstructions()** Handling Instruction | This service resolves the functionality associated with handling instructions for protected information annotated using Security Labels. | **Handling Instruction ] domainPolicy** |
| **completeFederatedPolicy()** Federated Security Policy | Once both domains resolve the constituent policies, the completed Federated Security Policy is approved and signed by each domain's representatives (e.g., Chief Security Officers). The new federated policy becomes part of the derived Trust Contract and is provisioned by both domains. | **Federated Security Policy ] domainPolicies** |
| **resolveDelegationPolicy()** Delegation Policy | None | **Delegation Policy ] delegation** |
| **resolveContextualPolicy()** Contextual Policy | None | **Contextual Policy ] contextual** |
| **resolveRefrainPolicy()** RefrainPolicy | None | **RefrainPolicy ] policy** |
| **resolveSecurityLabelDefinitions()** SecurityLabelDefinitions | None | **SecurityLabelDefinitions ] clientLabels** |

| Services | Notes | Parameters |
|---|---|---|
| **assertLevelOfAssurance()** int | None | **int ] level** |
| **getDomainAuthorizationPolicy()** Authorization Policy | None | |
| **getDomainPermissions()** Permission | None | |
| **getDomainRoles()** Roles | None | |
| **resolveHandlingFunctionality()** Functionality (HL7 EHRS FM) | None | **Handling Instruction ] caveats** |
| **resolveSecurityLabelingPolicy()** Composite Policy | None | **] domainPolicies** |

### 6.3 Domain A: CSO

Domain A's Chief Security Officer - this is an example stakeholder who may sign off and approve a Trust Contract (referenced in the signedBy [1..*] attribute).

### 6.4 Domain B: Enterprise Terminology Service

An Enterprise Terminology Service or Vocabulary Service establishes the formal value sets used by policy and by the technical frameworks that allow sharing data between domains. This service is critical to establishing semantic interoperability.

Specifically, this service identifies the value sets drawn from standard code systems - such as American Society for Testing and Materials (ASTM), SNOMED CT, LOINC, or HL7 - to be used including their version numbers. The selection of code sets should be consistent with the data in the exchange information objects. This ensures a common code set vocabulary between participants throughout the access request transaction. Use of different code sets and version numbers by participants in a transaction could lead to improper sharing or use of protected healthcare information.

### 6.5 National Registry

This is an example system that is capable of validating Technical Framework certification and Conformance Statements.


 

# APPENDIX A: Acronyms (Informative)

| Acronym | Term |
|---|---|
| ABAC | Attribute Based Access Control |
| ACI | Access Control Information |
| ACL | Access Control List |
| ACS | Access Control Service |
| ADI | Access Decision Information |
| ANSI | American National Standards Institute |
| AP | Attribute Provider |
| APS | Attribute Provider Statement |
| ASTM | American Society for Testing and Materials |
| AVM | Attribute Value Metadata |
| CCITT | International Telegraph and Telephone Consultative Committee |
| CDA | Clinical Document Architecture |
| CLINAST | Clinician Asserted |
| CNSSI | Committee on National Security Systems Instruction |
| CSP | Credential Service Provider |
| CRYPTOHASH | Cryptographic Hash Function |
| DAM | Domain Analysis Model |
| DIGSIG | Digital Signature |
| DRGIS | Drug Information Sensitivity |
| DS4P | Data Segmentation for Privacy |
| DURSA | Data Use and Reciprocal Support Agreement |
| EHNAC | Electronic Healthcare Network Accreditation Commission |
| EHR | Electronic Health Record |
| FBCA | Federal Bridge Certification Authority |
| FHIM | Federal Health Information Model |
| FHIR | Fast Healthcare Interoperability Resources |
| FISMA | Federal Information Security Management Act |
| GOV | Government |
| HCPAST | Healthcare Professional Asserted |
| HCS | Healthcare Classification System |
| HIV | Human Immunodeficiency Virus |
| HIMSS | Healthcare Information and Management Systems Society |
| HL7 | Health Level Seven |
| IDP | Identity Provider |


 

| Acronym | Term |
|---|---|
| IEC | International Electrotechnical Commission |
| IETF | Internet Engineering Task Force |
| INCITS | InterNational Committee for Information Technology Standards |
| ISO | International Organization for Standardization |
| ISTPA | The International Security, Trust, and Privacy Alliance |
| ITU | International Telecommunication Union |
| LOINC | Logical Observation Identifiers Names and Codes |
| NISTIR | National Institute of Standards and Technology Internal Report |
| OASIS | Organization for the Advancement of Structured Information Standards |
| PASS | Privacy, Access and Security Services |
| POU | Purpose of Use |
| RBAC | Role Based Access Control |
| REST | Representational State Transfer |
| RP | Relying Party |
| SAML | Security Assertion Markup Language |
| SLS | Security Labeling Service |
| SNOMED CT | Systematized Nomenclature of Medicine – Clinical Terms |
| SP | Service Provider |
| STS | Secure Trust Service |
| UMA | User Management Access |
| UML | Unified Modeling Language |
| URL | Uniform Resource Locater |
| VHA | Veterans Health Administration |
| XACML | eXtensible Access Control Markup Language |
| XML | Extensible Markup Language |


 

# APPENDIX B: Glossary of Terms (Informative)

| Term | Definition |
|---|---|
| Access | Performing an action. [XACML] |
| Access Control | Means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways. [ISO 2382-8]<br><br>Prevention of unauthorized use of a resource including the prevention of use of a resource in an unauthorized manner. [ISO 7498-2:1989]<br><br>Controlling access in accordance with a policy or policy set. [XACML] |
| Access Control Decision | Finite result of evaluating an access control policy for a given set of Access Control Information. [HL7 PASS ACS] |
| Access Control Decision Information (ADI) | The portion (possibly all) of the ACI associated with a principal or action that is made available for use in making a particular access control decision. [ISO 10181-3] |
| Access Control Information (ACI) | Information used for access control purposes. ACI may be associated with principals such as initiators or resources, may be associated with actions, and may include contextual information. [ISO 10181-3]<br><br>See also Contextual Information. |
| Access Control Mechanism | An access control mechanism is composed of an access control scheme and supporting mechanisms to provide access control decision information to an access control decision function for that scheme. Adapted from [ISO 10181-3] |
| Access Control Service (ACS) | The Access Control Service is the enterprise security service that supports and implements user-side and service-side access control capabilities. The service would be utilized by the Service and/or Service User. [ XACML] |
| Access Request | The operations and operands that form part of an attempted access. [ISO 10181-3] |
| Action | An operation on a Resource. [XACML] |
| Advice | A supplementary piece of information in a policy or policy set which is provided to the Policy Enforcement Point with the decision of the Policy Decision Point. [XACML] |
| Assertion | A statement from an attribute provider to a relying party that contains identity attributes about a subject. Assertions may also contain authentication or other identity information about the subject. [NISTR 8112] |
| Association | Symbols on Class diagrams used to associate the relationships between classes. They illustrate both how classes are associated as well as class inheritance between parent classes and sub classes. [UML] |
| Attribute | Characteristic of an initiator, resource, action or environment that may be |


 

| Term | Definition |
|---|---|
| | referenced in a predicate or target. [XACML]<br><br>A claim of a named quality or characteristic inherent in or ascribed to someone or something. [NISTR 8112]<br><br>Attributes are information related to user location, role, purpose of use, and requested resource requirements and actions necessary to make an access control decision. This terminology is used by the SAML and XACML specifications and is equivalent in concept to claims. [XSPA] |
| Attribute Based Access Control (ABAC) | Access control based on attributes associated with subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which access may take place. [NISTR 8112]<br><br>An access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environment conditions, and a set of policies that are specified in terms of those attributes and conditions. Attributes are characteristics of the subject, object, or environment conditions given by a name-value pair. The basic approach is where an ABAC Access Control Module (ACM) receives the subject's access request, and then examines the subject's and object's attributes against a specific policy. The ACM then determines what operations the subject may perform upon the object. For example, policy allows access to anyone who is 18 years or older. A requester with an assigned ages attribute value of 18 or greater is granted access. [NIST SP 800-162] |
| Attribute Claim (or "Claim") | A statement asserting a property of a subject without necessarily containing authentication or other identity information, independent of format. For example, for the attribute 'birthday', a claim could be 'older than 18' or 'born in December'. [NISTR 8112]<br><br>A statement made about a client, service or other resource (e.g., name, identity, key, group, privilege, capability, etc.). [WS-Trust] |
| Attribute Metadata | Data providing information about the context and structure of an attribute. See metadata. [NISTR 8112] |
| Attribute Provider (AP) | Manages and provides assertions of identity attributes to other relying and federated parties. [NISTR 8112] |
| Attribute Provider Statement (APS) | A document that captures the security, privacy, data protection, and attribute management practices of a given attribute provider or party acting as an attribute provider for a given set of transactions. [NISTR 8112] |
| Attribute Value Metadata (AVM) | Data describing an asserted value for an associated attribute. [NISTR 8112] |
| Authorization | The granting of rights, which includes the granting of access based on |


 

| Term | Definition |
|---|---|
| | access rights. [ISO 7498-2]<br><br>The granting of privileges, which includes the granting of privileges to access data and functions. [ISO 22600-2 – modified from ISO 7498 -2]<br><br>The decision to permit or deny a subject access to resources (e.g., network, data, application, services) based on the evaluation of access control policies. [NISTR 8112] |
| Blockchain | Blockchain is a transaction database shared by all nodes participating in a system. It is emerging as a way to make and verify transactions on a network instantaneously without a central authority. Blockchain technology supports various use cases such as (a) a distributed consensus needs to be established in the presence of malicious or untrustworthy actors, and (b) the need to electronically initiate and enforce contracts. |
| Break Glass | An administrative control which allows an authorized individual to access information under specific, declared circumstances. |
| Cardinality | A property that describes the size of the set by describing it using a number or an “unknown” indicator (*). |
| Child Class | Or subclass is a class that inherits some properties from its parent or superclass. |
| Claim | See Attribute Claim. |
| Class Diagram | The base UML diagram type is used for information modeling. Business Entities or nouns are represented as Classes on the diagram with attributes that describe their properties. Associations link Classes together with business rules that include cardinality, Associations roles and direction of flow. |
| Classification | Security label metadata that specifies the labeled resource’s level of confidentiality. [HL7 PASS SLS]<br><br>Confidential protection of data elements by segmentation into restricted and specifically controlled categories set by policies, professional practice, and laws, legislation, and regulations. [HL7 HCS adapted from ASTM E1986] |
| Clearance | Initiator-bound ACI that can be compared with security labels of targets. [ISO 10181-3]<br><br>Permission granted to an individual to access data or information at or below a particular security level. [ISO 2382-8] |
| Clearance Attribute | The clearance attribute is used to define the authorizations granted a specific user or application entity. [ITU X.841] |
| Compartment | Security label metadata that “segments” an IT resource by indicating that access and use is restricted to members of a defined community or project. |


 

| Term | Definition |
|---|---|
| | [HL7 HCS]<br><br>Compartment metadata assigned to a clinical fact that is conveyed in the Compartment "Named Tag Set", which is a type of Security Category label field in an HCS-conformant security label. [HL7 HCS]<br><br>Compartments encompass data items tagged for access to specific named groups. Being a member of the group is sufficient to determine access. Compartments provide broad access to information resource categories, but do not determine what fine-grained privileges a subject may have with respect to that resource (e.g., Role based access control). |
| Compartment Name Tag Set | Examples of compartments include, "For Pharmacy Personnel Only", "Agent Orange", and "Records Management". [HL7 HCS Vocab] |
| Conceptual Information Model (CIM) | A representation of an Information Model that only represents primary classes and associations and does not illustrate the attributes of the classes. |
| Condition | An expression of predicates. A function that evaluates to "True," "False" or "Indeterminate." [XACML] |
| Confidentiality | Security label metadata classifying an IT resource (clinical fact, data, information object, service, or system capability) according to its level of sensitivity, which is based on an analysis of applicable privacy policies and the risk of financial, reputational, or other harm to an individual or entity that could result if made available or disclosed to unauthorized individuals, entities, or processes. [HL7 HCS]<br><br>Classification metadata assigned to a clinical fact that is conveyed in the Confidentiality "Named Tag Set", which is a single valued, mandatory Security Classification label field in a HCS conformant security label. [HL7 HCS]<br><br>Confidentiality classifications are hierarchical levels in a multilevel policy that permits a user with a clearance classification equal to the classification label assigned to an information resource to "read down", i.e., to read less classified information objects, and to "write up", i.e., create information resources that are more highly classified, but does not permit the user to reclassify an information resource to a lower level of confidentiality. |
| Confidentiality Named Tag Set | Consists of the following: Unrestricted, Low, Moderate, Normal, Restricted, Very Restricted. [HL7 HCS Vocab] |
| Consent | Permission granted, withdrawn, or withheld by an individual, usually for the collection, access, use, or disclosure of personal information or individually identifiable health information for a given purpose. [HL7 PASS ACS] |


 

| Term | Definition |
|---|---|
| | The capability, including support for Sensitive Information, Informed Consent, Change of Use Consent, and Consequences of Consent Denial, provided to individuals to allow the collection and/or specific uses of some or all of their Personal Information either through an affirmative process (opt-in) or implied (not choosing to opt-out when this option is provided). [ISTPA] |
| Consent Directive | An instruction regarding consent to collect, use, and/or disclose Individually Identifiable Health Information. [HL7 PASS ACS]<br><br>A record of a Subject of Care's (e.g., patient, consumer) health information privacy policy. A Consent Directive grants or withholds authorization to collect, access, use, or disclose individually identifiable health information about the client. [HL7 CDA]<br><br>Think of a consent directive as a Subject of Care (e.g., Patient) specified set of access authorizations and refrains. A more detailed way to think of consent directive is a record of a healthcare consumer's policy choices, which permits or denies identified recipient(s) or recipient role(s) to perform one or more actions within a given policy context, for specific purposes and periods of time. |
| Constraint | A limitation on an access control rule. [HL7 PASS ACS]<br><br>Constraints can be specified to limit the applicability of policies based on time or values of the attributes of the objects to which the policy refers. [PONDER]<br><br>A limitation on the applicability of a policy. [XACML] Think of constraint as an "except" type rule. |
| Contextual Information | Information about or derived from the context in which an access request is made (e.g., time of day). [ISO 10181-3]<br><br>Contextual information might include source IP address, encryption strength, the type of operation being requested, time of day, etc. Portions of access control information may be specific to the request itself, others may be associated with the connection via which the request is transmitted, others (e.g., time of day) may be "environmental". [IETF RFC 2829] |
| Contract | See Trust Contract. |
| Credential Service Provider (CSP) | An entity that issues digital credentials to subjects and issues or registers authenticators for subjects' use. A CSP may be an independent third party or may issue credentials for its own use. A CSP may provide and verify attributes or may include attributes provided or verified by other entities. [NISTR 8112] |
| Data Blocking | The preventing, discouraging, or interfering with the access, exchange, or use of information. [Cures Act]. |


 

| Term | Definition |
|---|---|
| Data Use and Reciprocal Support Agreement (DURSA) | A comprehensive, multi-party trust agreement that is entered into voluntarily by public and private organizations (eHealth Exchange Participants) that desire to engage in electronic health information exchange with each other as part of the eHealth Exchange. The DURSA is based upon the existing body of law (Federal, state, local) applicable to the privacy and security of health information and is supportive of the current policy framework for health information exchange. The DURSA is intended to be a legally enforceable contract that represents a framework for broad-based information exchange among a set of trusted entities. [Sequoia Project] |
| Decision | The result of evaluating a rule, policy or policy set. [XACML] |
| Delegation | Conveyance of privilege from one entity that holds such privilege to another entity. [ISO 22600-2] |
| Discovery | Act of seeking and finding a target. [HL7 PASS ACS] |
| Domain | A distinct scope, within which certain common characteristics are exhibited and common rules observed. For example, a security policy domain is defined by the scope over which a security policy is enforced. There may be subdomains for different aspects of this policy. [OMG SEC]<br><br>See also Security Domain. |
| Domain Authority | A security authority that is responsible for the implementation of a security policy for a security domain. [ISO 10181-1] |
| Domain Characterization | A domain is characterized by a domain identifier, domain name, domain authority, and domain qualifier. [ISO 22600-2] |
| Domain Policy Framework | A description of the legal framework including rules and regulations, the organizational and administrative framework, functionalities, claims and objectives, the principals involved, agreements, rights, duties, and penalties defined, as well as the technological solution implemented for collecting, recording, processing, and communicating data in information systems. [ASTM E2595] |
| Effect | The intended consequence of a satisfied rule (either “Permit” or “Deny”). [XACML] |
| Encrypt | The process of changing plaintext into ciphertext for the purpose of security or privacy. [CNSSI 4009] |
| Entity | An entity may also be known as a principal and/or subject, which represents an application, a machine, or any other type of entity that may act as a requester in a transaction. [XSPA] |


 

| Term | Definition |
|---|---|
| Environmental Variables | Aspects of policy required for an authorization decision that are not contained within static structures, but are available through some local means to a privilege verifier (e.g. time of day or current account balance) [ISO 22600-2]<br><br>The set of attributes that are relevant to an authorization decision and are independent of a particular subject, resource or action. [XACML] |
| Federal Health Information Model (FHIM) | The Federal Health Information Model is an effort originated and managed by the Office of National Coordinator under Health and Human Services to create a high-level information model that models and standardizes metadata of health information domains across the federal health information community." [FHIM] |
| Federated Domain | A Federated Domain is a collection of domains that have established a producer-consumer relationship whereby one domain can provide authorized access to a resource it manages to an entity in another domain requesting access. This is accomplished via run-time derivation of trust and access control policies, and the conveyance of access control attributes.<br><br>A domain operating under policies of trust such that one member may make requests for, and then receive protected information from another.<br><br>Federated authorization is a subset of the broader federation concept that, per [WS-Federation] includes the brokering of identity, attribute, authentication and authorization assertions between domains. A Federated Domain assumes that any necessary identity brokering has been successfully completed prior to the authorization/access processing. |
| Federated Policy Domain | In a federation, each domain retains most of its authority while agreeing to afford the other limited rights.<br>• The federation agreement records:<br>• The rights given to both sides, such as the kind of access allowed.<br>• The trust each has in the other.<br>It includes an agreement as to how policy differences are handled, for example, the mapping of roles in one domain to roles in the other. [OMG SEC] |
| Federation | A process that allows for the conveyance of identity attributes and authentication information across a set of networked systems. [NISTR 8112]<br><br>A federation is a collection of domains that have established a producer-consumer relationship whereby one domain can provide authorized access to a resource it manages based on an identity, and possibly associated attributes, that are asserted in another domain. Federation requires trust such that a Relying Party can make a well-informed access control decision based on the credibility of identity and attribute data that is |


 

| Term | Definition |
|---|---|
| | vouched for by another domain. Federation provides mechanisms that enable the decision to be based on the declaration (or brokering) of identity, attribute, authentication and authorization assertions between domains. [WS-Federation] |
| Functional Role | Functional roles reflect functional aspects of relationships between entities. Functional roles are bound to the realization/performance of acts, where actions might be concatenated to an activity or even to a process. [ISO 22600-2] |
| Group | A group is a set of Initiators whose members are considered equivalent when a particular access control policy is enforced. Groups allow access to particular Resources by a set of Initiators without the necessity of including the identity of individual Initiators in a Resource's ACI, and without explicitly allocating the same ACI to each Initiator. Access control policies stated in terms of groups of initiators are particular types of identity-based policies. [ISO 10181-3] |
| Handling Instructions<br><br>(Handling Caveats) | Security label metadata conveys dissemination controls and information handling instructions such as obligations and refrain policies to which a resource custodian or receiver must comply. This type of handling caveat must be assigned to a clinical fact if required by jurisdictional or organizational policy, which may be triggered by a Subject of Care consent directive. [HL7 HCS]<br><br>Handling caveat metadata assigned to a clinical fact that is conveyed in a Handling Caveat "Named Tag Set", which is a type of Security Category label field in a HCS conformant security label. [HL7 HCS] |
| HL7 Reference Information Model (RIM) | The high-level canonical information model that is at the root of HL7 version 3's information model. Every effort is being made to stay in close alignment with the HL7 modeling style and organization. |
| HL7 Security and Privacy Domain Analysis Model (DAM) | The DAM contains a harmonized analysis of the security and privacy system requirements of healthcare organizations and their clients and is intended to meet these challenges by identifying the information and system behaviors required to implement technological controls enforcing healthcare security and privacy policy. The model is intended to support the reuse of security standards to enforce access control policies required by jurisdictional and organizational privacy policies as well as individual client consent directives. It focuses on the information required to support authorization and access control use cases. [HL7 DAM] |
| Identity Provider (IDP) | A Credential Service Provider (CSP) in a federation that manages the subject's primary authentication credentials and issues assertions derived from those credentials. [NISTR 8112] |
| Individually Identifiable Health Information | Health Information that contains or can be reconstituted to refer to a specific, identifiable individual. [HL7 PASS ACS] |
| Information Model | An information model is a representation of concepts, relationships, constraints, rules, and operations to specify data semantics for a chosen domain of discourse. The advantage of using an information model is that |


 

| Term | Definition |
|---|---|
| | it can provide sharable, stable, and organized structure of information requirements for the domain context [Info Model].<br><br>In other words, an information model is an abstract representation of a subject area of interest designed to provide a generic representation of a class of system or capability and to suggest a set of approaches to implementation. |
| Initiator | An entity (e.g., human user or computer-based entity) that attempts to access other entities. [ISO 10181-3] |
| Integrity | Security label metadata that "segments" a resource by conveying the completeness, veracity, reliability, trustworthiness, and provenance of the resource. [HL7 PASS SLS]<br><br>Integrity metadata assigned to a clinical fact that is conveyed in the Integrity "Named Tag Set", which is a type of Security Category label field in a HCS conformant security label. [HL7 HCS]<br><br>A property that information is not altered in any way, deliberately or accidentally. [ISO 22600-2]<br><br>The property that data has not been altered or destroyed in an unauthorized manner. [ISO 10181-1] |
| Inter-domain communication and cooperation | Interoperability between domains is called an inter-domain communication and co-operation. [ISO 22600-1]<br><br>See also Security Domain. See also Interoperability. |
| Intra-domain communication and cooperation | Any kind of interoperability internally to a domain is called an intra-domain communication and co-operation. [ISO 22600-1]<br><br>See also Security Domain. See also Interoperability. |
| Interoperability | Ability to coordinate operations in a meaningful way. [HL7 PASS ACS] |
| Jurisdictional Policy | Class of policy used to represent a territorial authority that may be issuing privacy and/or security policies for a territory. [HL7 DAM] |
| Mask | Encrypt segments of protected information so that they are inaccessible without access to decryption keys. [HL7 HCS] |
| Metadata | Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about information or information about information. [NISTR 8112] |
| Multi-domain Information Object<br>(aka Compound Object) | A collection of objects from different security domains perceived by users as a single information object. In compound security domains, additional policies shall be written that apply to the newly created multidomain information objects. The multidomain information security policy shall |


 

| Term | Definition |
|---|---|
| | state the privileges that a user must have to view, print, create, delete, or transfer multidomain information objects between information systems. It cannot be assumed that the compound domain policies are simply inherited from the subdomains. [ASTM E2595]<br><br>The reference model allows an object reference to be a member of multiple domains, which may overlap for the same type of policy (for example, be subject to overlapping access policies). This would require conflicts among policies defined by the multiple overlapping domains to be resolved. The specification does not include explicit support for such overlapping domains and, therefore, the use of policy composition rules required to resolve conflicts at policy enforcement time. [OMG SEC] |
| Object | Any system resource subject to access control, such as a file, printer, terminal, database record. [HL7 PASS ACS]<br><br>Members of a domain. [OMG SEC]<br><br>An entity that contains or receives information. [ANSI 359-2004] |
| Obligation | Constraint dealing with required behavior. [HL7 PASS ACS]<br><br>Actions to be performed. [ISO 22600-2]<br><br>An operation specified in a rule, policy, or policy set that should be performed by the Policy Enforcement Point in conjunction with the enforcement of an authorization decision. [XACML] |
| Operation | An operation is an executable image of a program, which upon invocation executes some function for the user. Within a file system, operations might include read, write, and execute. Within a database management system, operations might include insert, delete, append, and update. An operation is also known as an action or privilege. [ANSI 359-2004] |
| Organizational Policy | Class of policy used to represent an organization that may be issuing privacy and/or security policies. [HL7 DAM] |
| Parent Class | Also known as superclass, Parent Class is a class from which other classes are derived. The classes that are derived from a superclass are known as child classes, derived classes, or subclasses. [UML] |
| Patient Consent | See Consent |
| Patient Correlation<br><br>(Patient Matching) | The accurate and efficient matching of patients to their health records. Matching patients to their records is a foundational component of electronic health information exchange. Incorrect matching can result in misinformation and medical error and can compromise privacy and security if patient information is inappropriately disclosed. A patient's health information may have multiple identifiers within a single institution or multiple identifiers across multiple institutions. This fragmented environment makes it difficult to correctly link information about individuals when it is needed for clinical and health care functions. [HealthIT] |


 

| Term | Definition |
|---|---|
| Permission | An operation on an object. [ANSI 359-2004]<br><br>A scope of access over a particular resource set at a particular resource server that is being requested by, or granted to, a requesting party. [UMA]<br><br>An approval to perform an operation on one or more RBAC protected objects. [ANSI 359-2004] |
| Policy | A set of legal, political, organizational, functional and technical obligations for communication and cooperation. [ISO 22600-2]<br><br>The formulation of the concept of requirements and conditions for trustworthy creation, collection, storage, processing, disclosure, retention, transmission, and use of sensitive information. [ISO 22600-2]<br><br>The rules and criteria that constrain activities of the objects to make the domain secure. [OMG SEC]<br><br>A set of rules, an identifier for the rule-combining algorithm and (optionally) a set of obligations. May be a component of a policy set. [XACML]<br><br>A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users. [ITU X.800] |
| Policy Bridging | Policy bridging is the process used to derive (negotiate) the set of common, domain-specific security and privacy policies required for trustworthy co-operation between collaborating domains. Derived from [ISO 22600-1] |
| Policy Component | The composition or decomposition according to the generic component model. Using HL7 version 3 data type definitions, the policy class can be specialized into basic policy, meta policy and composite policy. (Derived from ISO 22600-2) |
| Policy Set | A set of policies, other policy sets, a policy-combining algorithm and (optionally) a set of obligations or advice. May be a component of another policy set. [XAMCL] |
| Predicate | A statement about attributes whose truth can be evaluated. [XACML] |
| Provenance | Provenance refers to attributes about the origin of health information at the time it is first created and tracks the uses and permutations of the health information over its lifecycle. [S&I Framework]<br><br>Provenance of a resource is a record that describes entities and processes involved in producing and delivering or otherwise influencing that |


 

| Term | Definition |
|---|---|
| | resource. Provenance provides a critical foundation for assessing authenticity, enabling trust, and allowing reproducibility. Provenance assertions are a form of contextual metadata and can themselves become important records with their own provenance. [W3C Provenance] |
| Purpose of Use | Purpose of Use is typically asserted by the information requester or on a query parameter. Just like other access control information such as subject role, resource type, time, or location of access, purpose of use can also be a factor in defining policy rules and be the basis of permitting or denying the request or triggering obligations and advices. [HL7 DAM]<br><br>Security label metadata that indicates the stated intent for access to privacy data. [HL7 PASS ACS]<br><br>Reason for performing one or more operations on information, which may be permitted by source system's security policy in accordance with one or more privacy policies and consent directives. [HL7 HCS Vocab]<br><br>Usage Notes: The rationale or purpose for an act relating to the management of personal health information, such as collecting personal health information for research or public health purposes. [HL7 HCS Vocab] |
| Redact | Remove content from the response, making it impossible to recover regardless of permissions. [HL7 HCS] |
| Refrain | Actions the subjects must refrain from performing. [ISO 22600-2] Think of refrain as a restriction – something that the subject is not allowed to do. |
| Relying Party (RP) | An entity that relies upon a subject's authenticator(s) and credentials or an IDP's assertion of a subject's identity, typically to process a transaction or to grant access to information or a system. [NISTR 8112] |
| Resource | An entity to which access may be attempted. [ISO 10181-3] |
| Retained Access Control Decision Information (ADI) | ADI which has been retained from earlier access control decisions for use in future access control decisions. [ISO 10181-3] |
| Role | A role groups the policies specifying the duties and rights relating to a position within an organization. A role is thus a particular type of group in which all policies have the same subject domain. A role can contain basic policies and groups of basic policies but not nested roles, relationships or management structures. The role instantiation declaration may specify an optional path name, which is to be used as the subject domain for the role. This assumes the subject domain has already been created in the domain hierarchy. If the subject domain is not specified then a domain with the name of the role instance is implicitly created and used as the subject domain i.e. the subject for policies within the role. [PONDER]<br><br>A role characterizes the functions a user is allowed to perform within an |


 

| Term | Definition |
|---|---|
| | organization. A given role may apply to a single individual (e.g., director of a department) or to several individuals (e.g., teller, loan officer, member of a board). Access control policies stated in terms of initiators acting in specific roles are particular types of identity-based policies. [ISO 10181-3] |
| Role Based Access Control (RBAC) | A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities. [XACML RBAC] |
| Rule | A target, an effect, a condition and (optionally) a set of obligations or advice. A component of a policy. [XACML] |
| Rule Based Security Policy | A security policy based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users. [ITU X.800] |
| Rule-combining Algorithm | The procedure for combining decisions from multiple rules. [XACML] |
| Security Authority | A security authority must be identifiable and responsible for defining the policies to be applied to the domain but may delegate that responsibility to a number of sub-authorities, forming subdomains where the subordinate authorities' policies are applied. Subdomains may reflect organizational subdivisions or the division of responsibility for different aspects of security. Typically, organization-related domains will form the higher-level superstructure, with the separation of different aspects of security forming a lower-level structure. [OMG SEC] |
| Security Category | Components of Healthcare Classification System (HCS)Security Labels are designated as either restrictive or permissive tags according to whether a clearance must meet all the category tags in a clinical fact label (restrictive) or whether a clearance must only meet one category tags in order to gain access. [HL7 HCS]<br><br>The HCS Security Category Named Tag Set may include multiple Tag Set Name fields for the different Security Categories such as Sensitivity, Compartment, Privacy Policies and Laws, Integrity, and Provenance. Each Security Category Name Tag Set field includes one or more security tags valuing the label field. [HL7 HCS] |
| Security Classification | The determination of which specific degree of protection against access the data or information requires, together with a designation of that degree of protection. [HL7 HCS]<br><br>Healthcare Classification System (HCS) Security Classification Named Tag Set contains only one Tag Set Name, Confidentiality. [HL7 HCS]<br><br>The tags with which the HCS Security Classification Tag Set Name may be valued are the codes in the HL7 Confidentiality code system. [HL7 HCS] |
| Security Control | The Healthcare Classification System (HCS) Security Control Name Tag Set may include multiple Tag Set Name fields for the handling caveats applicable to the labeled clinical fact based on the privacy and security |


 

| Term | Definition |
|---|---|
| | policies governing access and disclosure of the labeled clinical fact. [HL7 HCS] |
| Security Domain | A set of subjects, their information objects, and a common security policy. [NIST SP 800-33]<br><br>Security Domain Attributes:<br>• Within a security domain, all information objects exist at the same level of sensitivity [ASTM2595]. Note: this is synonymous with the "confidentiality classification" found in [HL7 HCS].<br>• Members of a domain may have different security attributes, such as read, write, or execute permissions on information objects. [ASTM2595]<br>• Security domains are not bound by systems or networks of systems. [ASTM2595]<br><br>A security domain's objects may reside in multiple systems. [ASTM2595]<br><br>Set of elements, a security policy, a security authority and a set of security-relevant activities in which the set of elements are subject to the security policy for the specified activities, and the security policy is administered by the security authority for the security domain. The activities of a security domain involve one or more elements from that security domain and, possibly, elements of other security domains. [ISO 10181-1]<br><br>A collection of users and systems subject to a common security policy. [ITU X.841]<br><br>To keep information systems that support Shared Care manageable and operating, principal-related components of the system are grouped by common organizational, logical, and technical properties into domains. Any kind of interoperability internally to a domain is called an intra-domain communication and co-operation, whereas interoperability between domains is called an inter-domain communication and co-operation. For example, communication could be realized between departments of a hospital internally to the domain hospital (intra-domain communication), or externally to the domain of a special department (inter-domain communication). A domain might consist of sub-domains (which will inherit and might specialize policies from the parent domain). The smallest-scale domain might be an individual workplace or a specific component within an information system. Domains can be extended into super-domains, by chaining a set of distinct domains and forming a common larger-scale domain for communication and co-operation. A domain is characterized by a domain identifier, domain name, domain authority, and domain qualifier. [ISO 22600-2:2006]<br><br>A single unit of security administration or trust. [WS-Federation] |


 

| Term | Definition |
|---|---|
| Security Label | Security labels are meta-data conveying constraints on the use of a labeled Resource, which are used as Resource access control decision information to match against an Initiator's (i.e., service requester's) clearance in order to render an access decision with the applicable obligations required by policy. [HL7 PASS SLS]<br><br>Access control policies stated in terms of security labels are particular types of rule-based security policies. Initiators and targets are separately associated with named security labels. Access decisions are based on a comparison of the initiator and target security labels. These policies are expressed by rules describing which accesses may take place between initiators and targets with specified security labels. [ISO 10181-3] |
| Security Policy | The complex of legal, ethical, social, organizational, psychological, functional, and technical rules for ensuring trustworthiness of health information systems. [ISO 22600-2]<br><br>A security policy expresses security requirements for a security domain in general terms. For example, a security policy may identify requirements that apply to all members of a security domain when operating under specific conditions, or that apply to all information in a security domain. The implementation of a security policy will result in security services being identified that will satisfy the security policy, and security mechanisms will be chosen to implement the security services. A security policy constrains the activities of elements subject to that security policy, either by requiring certain actions or by prohibiting certain activities. [ISO 10181-1] |
| Security Policy Domain | A set of objects to which a security policy applies for a set of security related activities and is administered by a security authority. (Note that this is often just called a security domain and are here treated as equivalent.) The objects are the domain members. The policy represents the rules and criteria that constrain activities of the objects to make the domain secure. [OMG SEC] |
| Security Policy Information File (SPIF) | A construct that conveys domain-specific security policy information. The Security Policy Information File is a signed object to protect it from unauthorized changes. [ITU X.841]<br><br>A security labelling policy is often represented in a file, referred to as a SPIF (Security Policy Information File). A key benefit of using a SPIF is that it provides an electronic representation of the complete security labelling policy in one place that can be shared and installed on systems that need to implement the security labelling policy. [Open XML SPIF]<br><br>An XML schema, that provides a high-level representation of a security classification policy in a generic and open fashion. [Open XML SPIF]<br><br>A SPIF is a file representation of the Security Policy (i.e., the definition of |


 

| Term | Definition |
|---|---|
| | which Security Labels are valid and how to check them against Security Clearances). The basic concept is simple, although the details get more complex because of the desire to support complex Security Policy. By abstracting Security Policy into a SPIF, this definition becomes separate from the product that enforces or supports the Security Policy. [ISODE] |
| Security Service | A service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers. [ITU X.800] |
| Security Token | Construct that represents a collection of statements (claims) made about a client, service or other resource [WS-TRUST]. Examples of statements/claims are name, identity, group, privilege, capability, Trustmark Provider used, Technical Framework used, Data Use Agreement used.<br><br>A set of data protected by one or more security services, together with security information used in the provision of those security services, that is transferred between communicating entities. [ISO 10181-1]<br><br>A packaged collection of data meant to be transmitted to another entity. A token could be used for authorized access (an "access token") or could be used to exchange information about a subject (a "claim token"). [UMA] |
| Secure Trust Service (STS) | A Secure Trust Service (STS) is a Web service that issues security tokens. That is, it makes assertions based on evidence that it trusts, to whoever trusts it (or to specific recipients). To communicate trust, a service requires proof, such as a signature, to prove knowledge of a security token or set of security token. A service itself can generate security tokens or it can rely on a separate STS to issue a security token with its own trust statement (note that for some security token formats this can just be a re-issuance or co-signature). This forms the basis of trust brokering. [WS-Trust]<br><br>In this framework, the STS supports tokens or trustmarks required for trust and policy federation across domains including tokens asserting currently certified capabilities. Certified refers to conformance to a well-defined set of requirements specified for that capability. The requirements derive from a recognized, trustmark defining organization. |
| Semantic Interoperability | Provides interoperability at the highest level, which is the ability of two or more systems or elements to exchange information and to use the information that has been exchanged. Semantic interoperability takes advantage of both the structuring of the data exchange and the codification of the data including vocabulary so that the receiving information technology systems can interpret the data. This level of interoperability supports the electronic exchange of patient summary information among caregivers and other authorized parties via potentially disparate electronic health record (EHR) systems and other systems to improve quality, safety, efficiency, and efficacy of healthcare delivery. [HIMSS] |
| Sensitivity | The characteristic of a resource which implies its value or importance and may include its vulnerability. [HL7 HCS]<br><br>Security label metadata that "segments" a resource by conveying the |


 

| Term | Definition |
|---|---|
| | completeness, veracity, reliability, trustworthiness, and provenance of the resource (e.g., anonymized, signed, Subject of Care reported). [HL7 PASS SLS]<br><br>Privacy metadata for information perceived as undesirable to share:<br>• Sensitive information is data that must be protected from unauthorized access and disclosure to safeguard the privacy or security of an individual or organization.<br>• Classification is the act or process by which information is determined to be sensitive or non-sensitive.<br>• The appropriate classification level is determined by the disclosure risks of the information, which usually are identified by the magnitude, amount or kind of damage that could be caused by disclosure. [HL7 HCS]<br><br>Sensitivity metadata assigned to a clinical fact that is conveyed in the Sensitivity "Named Tag Set", which is a type of Security Category label field in a HCS conformant security label. [HL7 HCS] |
| Sensitivity Named Tag Set | Examples of sensitivity values: HIV, Sickle Cell Disease, VIP, Substance Abuse, Mental Health, Generic. [HL7 HCS Vocab] |
| Service Provider (SP) | The service provider represents the system providing a protected resource and relies on the provided security service. [XSPA] |
| Service User | The service user represents any individual entity [such as on an Electronic Health Record (EHR)/Personal Health Record (PHR) system] that needs to make a service request of a Service Provider. [ XSPA] |
| Structural Role | Structural roles reflect the structural aspects of relationships between entities. Structural roles describe prerequisites, feasibilities, or competencies for acts. [ISO 22600-2]<br><br>A job function within the context of an organization whose permissions are defined by operations on workflow objects. [ISO 21298] |
| Subdomain | A domain completely enclosed within the scope of a larger domain. [ASTM E2595]<br><br>A domain might consist of subdomains (which will inherit and might specialize policies from the parent domain). The smallest-scale domain might be an individual workplace or a specific component within an information system. [ISO 22600-2]<br><br>A security authority must be identifiable and responsible for defining the policies to be applied to the domain but may delegate that responsibility to a number of sub-authorities, forming subdomains where the subordinate authorities' policies are applied. Subdomains may reflect organizational subdivisions or the division of responsibility for different aspects of security. Typically, organization-related domains will form the higher-level superstructure, with the separation of different aspects of security |


 

| Term | Definition |
|---|---|
| | forming a lower-level structure. [OMG SEC]<br><br>Security domain A is said to be a security subdomain of another security domain B if, and only if:<br>• the set of elements of A is a subset of, or is the same as, the set of elements of B;<br>• the set of activities in A is a subset of, or is the same as, the set of activities in B;<br>• jurisdiction for A is delegated from the security authority of B to the security authority of A; and<br>• the security policy of A does not conflict with the security policy of B. A may introduce additional security policy if required, and if permitted by the security policy of B. [ISO 10181-1] |
| Subject | Person to whom data pertains. [HL7 PASS ACS] |
| Subject of Care | One or more persons scheduled to receive, receiving, or having received a health service. [ISO 27799] |
| Superdomain | Domains can be extended into super-domains, by chaining a set of distinct domains, forming a common larger-scale domain for communication and co-operation. [ISO 22600-2]<br><br>Security domain A is said to be a *security superdomain* of another security domain B if and only if B is a security subdomain of A. [ISO 10181-1]<br><br>An extended domain formed by chaining subdomains into a common domain of communication and cooperation that is characterized by an agreed upon security policy. [ASTM E2595] |
| Syntactic (Structural) Interoperability | An intermediate level that defines the structure or format of data exchange (i.e., the message format standards) where there is uniform movement of healthcare data from one system to another such that the clinical or operational purpose and meaning of the data is preserved and unaltered. Structural interoperability defines the syntax of the data exchange. It ensures that data exchanges between information technology systems can be interpreted at the data field level. [HIMSS] |
| Syntax | In logic, syntax is anything having to do with formal languages or formal systems without regard to any interpretation or meaning given to them. Syntax is concerned with the rules used for constructing, or transforming the symbols and words of a language, as contrasted with the semantics of a language which is concerned with its meaning.<br><br>In computer science, the syntax of a computer language is the set of rules that defines the combinations of symbols that are considered to be a correctly structured document or fragment in that language. |
| Target | Resource being accessed. [ISO 22600-2]<br><br>An entity to which access may be attempted. [ISO 10181-3] |

| Term | Definition |
|---|---|
| | An element of an XACML rule, policy, or policy set which matches specified values of resource, subject, environment, action, or other custom attributes against those provided in the request context as a part of the process of determining whether the rule, policy, or policy set is applicable to the current decision. [XACML] |
| Token | See Security Token |
| Transport (Foundational) Interoperability | Allows data exchange from one information technology system to be received by another and does not require the ability for the receiving information technology system to interpret the data. [HIMSS] |
| Trust | [ISO 22600-2]. In other words, trust defines the individual expectations in the context of the collection, processing, communication and use of personal information. It allows acceptance of risk and balancing privacy needs against benefits.<br><br>Trust is the characteristic whereby one entity is willing to rely upon a second entity to execute a set of actions and/or to make a set of assertions about a set of principles and/or digital identities. In the general sense, trust derives from some relationship (typically a business or organizational relationship) between the entities. [WS-Federation]<br><br>Circumstance existing between two entities whereby one entity makes the assumption that the other entity will behave exactly as the first entity expects<br><br>Entity X is said to trust entity Y for a set of activities if and only if entity X relies upon entity Y behaving in a particular way with respect to the activities. [ISO 10181-1] |
| Trust Bundle | A “trust bundle” is a collection of anchor certificates from health information service providers (HISPs) that comply with a baseline set of common policies and practices. This eliminates the need for participating HISPs to manually exchange and maintain trust anchors with each other. |
| Trust Context | The environmental, legal, social, and technical components of a Federated Domain. |
| Trust Contract | Sets of rules followed by the parties involved for achieving interoperability. [Based on ISO 22600-1] |
| Trust Framework | The Trust Framework facilitates trustworthy co-operation between domains by defining a common set of security and privacy policies that applies to all collaborating entities, derived from the relevant domain-specific policies across all of those policy domains. [Based on ISO 22600-2]<br><br>The “rules” underpinning federation, typically consisting of system, legal, conformance, and recognition. [NISTIR 8149] |


 

| Term | Definition |
|---|---|
| Trust Policy | Pre-contract policy element. A list of capabilities that an entity can assert in establishing a trust contract.<br><br>A mandate, obligation, requirement, rule, or expectation conveyed as security metadata between senders and receivers required to establish the reliability, authenticity, and trustworthiness of their transactions. [ISO 10181-1] and [NIST SP 800-63-3]<br><br>Trust security metadata are observations made about aspects of trust applicable to an IT resource (data, information object, service, or system capability). [ISO 10181-1] and [NIST SP 800-63-3]<br><br>Trust applicable to IT resources is established and maintained in and among security domains and may be comprised of observations about the domain's trust authority, trust framework, trust policy, trust interaction rules, means for assessing and monitoring adherence to trust policies, mechanisms that enforce trust, and quality and reliability measures of assurance in those mechanisms. Based on [ISO 10181-1] and [NIST SP 800-63-3] |
| Trusted Entity | An entity that can violate a security policy, either by performing actions which it is not supposed to do, or by failing to perform actions which it is supposed to do. [ISO 101-81-1] |
| Trusted Third Party | A security authority or its agent that is trusted with respect to some security-relevant activities (in the context of a security policy). [ISO 10181-1] |
| Trustmark | A Trustmark is a machine-readable, cryptographically signed digital artifact, issued by a Trustmark Provider to a Trustmark Recipient, and relied upon by one or more Trustmark Relying Parties. A Trustmark represents an official attestation by the Trustmark Provider of conformance by the Trustmark Recipient to a well-defined set of requirements and assessment criteria pertaining to trust and/or interoperability for the purpose of interaction with and use of digital information resources and services. A Trustmark Relying Party may rely upon a Trustmark as the basis for third-party trust in the Trustmark Recipient with respect to the set of requirements represented by the Trustmark. [GTRI]<br><br>Like compliance marks, trustmarks are a visual indication that a service provider is compliant with a federation's requirements. Trustmarks comprise a very specific subset of compliance marks. In addition to being electronically verifiable, these logos or seals are backed by rigorous third-party validation, assessment, or auditing. Certification of conformance and associated trustmarks may be issued by the assessor, the federation, or a separate certifying body on behalf of the federation. The key point is that certification trustmarks result from independent 3rd- party assessments and both the assessing and the certifying organizations stand behind the certifications with their own brand name and reputation. Therefore, trustmarks serve as a reliable and high assurance means to convey compliance with federation rules. [NISTIR 8149] |


 

| Term | Definition |
|---|---|
| Unified Modeling Language (UML) | Language for modeling software related requirements. There are 7 different models for communicating different aspects of software ranging from UI to data objects. UML Class Diagrams are the preferred model type used to document information models in the Business Information Architecture. |
| User | A consumer of the services offered by an RP. [NISTIR 8149] |
| Vocabulary | Language terms pertaining to a domain of discourse. [HL7 PASS ACS] |
| Web Service | The service user represents any individual entity [such as on an Electronic Health Record (EHR)/Personal Health Record (PHR) system] that needs to make a service request of a Service Provider. [XSPA] |
| XML | Extensible Markup Language (XML) is a simple, very flexible text format derived from SGML (ISO 8879). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety of data on the Web and elsewhere. [W3C XML] |


 

# APPENDIX C: References (Informative)


| | |
|---|---|
| [42 CFR Part 2] | Electronic Code of Federal Regulations (CFR) 42 Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5;node=42%3A1.0.1.1.2 |
| [ActPrivacyLaw] | HL7 v3 Code System ActUSPrivacyLaw https://www.hl7.org/fhir/v3/ActUSPrivacyLaw/index.html |
| [ANSI 359-2004] | ANSI/INCITS 359-2004; Information Technology - Role Based Access Control https://www.ansi.org/ |
| [ASTM E1986] | ASTM E1986; Standard Guide for Information Access Privileges to Health Information https://www.astm.org/Standards/E1986.htm |
| [ASTM E2595] | ASTM E2597; 2007; Standard Guide for Privilege Management Infrastructure https://www.astm.org/Standards/E2595.htm |
| [CCIT X.800] | CCIT X.800 \| ISO 7498-2: Security Architecture for Open Systems Interconnection for CCITT Applications https://www.itu.int/rec/T-REC-X.800-199103-I/en |
| [CNSSI 4009] | Committee on National Security Systems Instruction 4009; National Information Assurance (IA) Glossary https://www.ecs.csus.edu/csc/iac/cnssi_4009.pdf |
| [Cures Act] | H.R.34 - 21st Century Cures Act; 114th Congress (2015-2016) https://www.congress.gov/bill/114th-congress/house-bill/34/ |
| [FHIM] | Federal Health Information Model; Security and Privacy package (FHIM) http://www.fhims.org/content/420A62FD03B6_root.html |
| [GTRI] | Georgia Tech Research Institute (GTRI); Trustmark Framework Technical Specification v1.1 https://trustmark.gtri.gatech.edu/specifications/trustmark-framework/1.1/tfts-1.1.pdf |
| [HealthIT] | HealthIT.gov; Privacy and Security Solutions for Interoperable Health Information Exchange: Perspectives on Patient Matching: Approaches, Findings, and Challenges; Prepared for the Office of Policy and Research, Office of the National Coordinator for Health IT https://www.healthit.gov/sites/default/files/patient-matching-white-paper-final-2.pdf |
| [HIMSS] | Healthcare Information and Management Systems Society, What is Interoperability http://www.himss.org/library/interoperability-standards/what-is-interoperability |
| [HL7 CDA] | HL7 Clinical Document Architecture http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7 |
| [HL7 CDA Consent] | HL7 Implementation Guide for Clinical Document Architecture: Consent Directives http://www.hl7.org/implement/standards/product_brief.cfm?product_id=280 |

| | |
|---|---|
| [HL7 DAM] | HL7 Domain Analysis Model: Composite Security and Privacy (HL7 DAM); 2014<br>http://www.hl7.org/index.cfm?ref=nav |
| [HL7 DS4P] | HL7 Implementation Guide: Data Segmentation for Privacy (DS4P), Release 1 (HL7 DS4P)<br>http://www.hl7.org/index.cfm?ref=nav |
| [HL7 HACC] | HL7 Version 3 Standard: Healthcare (Security and Privacy) Access Control Catalog, Release 3<br>http://www.hl7.org/implement/standards/product_brief.cfm?product_id=72 |
| [HL7 HCS] | HL7 Healthcare Privacy and Security Classification System (HCS); 2014<br>http://www.hl7.org/implement/standards/product_brief.cfm?product_id=345 |
| [HL7 HCS Vocab] | HL7 Healthcare Privacy and Security Classification System (HCS); Security Label Vocabulary; 2014<br>http://www.hl7.org/implement/standards/product_matrix.cfm?ref=nav |
| [HL7 PASS ACS] | HL7 Version 3 Standard: Privacy, Access and Security Services (PASS) - Access Control, Release 1<br>http://www.hl7.org/index.cfm?ref=nav |
| [HL7 PASS SLS] | HL7 PASS Security Labeling Service (HL7 PASS SLS), 2014<br>http://www.hl7.org/index.cfm?ref=nav |
| [HL7 PFL] | HL7 Patient-friendly Language for Security and Privacy for Consent Directives<br>http://www.hl7.org/special/committees/projman/searchableprojectindex.cfm?action=edit&ProjectNumber=1130 |
| [HL7 PSAF] | HL7 Privacy and Security Architecture Framework<br>http://www.hl7.org/special/committees/projman/searchableprojectindex.cfm?action=edit&ProjectNumber=914 |
| [HL7 RBAC Engineer] | HL7 RBAC Engineering concepts<br>http://www.hl7.org/index.cfm?ref=nav |
| [HL7 Role Constraint] | HL7 Role Based Access Control Constraint Catalog<br>https://webcache.googleusercontent.com/search?q=cache:ffVREl8n92cJ:https://www.hl7.org/documentcenter/public/wg/secure/HL7%2520Constraints.doc+&cd=1&hl=en&ct=clnk&gl=us |
| [IETF RFC 1457] | Security Label Framework for the Internet; 1993<br>https://tools.ietf.org/html/rfc1457 |
| [IETF RFC 2829] | Authentication Methods for LDAP<br>https://www.ietf.org/rfc/rfc2829.txt |
| [IETF UMA Spec] | User Managed Access (UMA) Profile of OAuth 2.0; 2015<br>https://docs.kantarainitiative.org/uma/rec-uma-core.html |
| [Info Model] | Information Modeling: From Design to Implementation; National Institute of Standards and Technology (NIST); Tina Lee;<br>http://www.mel.nist.gov/msidlibrary/doc/tina99im.pdf |
| [ISO 10181-1] | ISO/IEC International Standard 10181-1:1996; Data Networks and Open System Communications – Security<br>https://www.itu.int/rec/T-REC-X.810-199511-I/en |

| | |
|---|---|
| [ISO 10181-3] | ISO/IEC 10181-3:1996; Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework http://www.iso.org/iso/catalogue_detail.htm?csnumber=18199 |
| [ISO 13606-5] | ISO/IEC 13606-5:2010; Health Informatics – Electronic Health Record Communication – Part 4: Security http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50121 |
| [ISO 15816] | ISO/IEC 15816:2002; Security Information Objects for Access Control http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=29139 |
| [ISO 21298] | ISO 21298:2017 Health Informatics - Functional and Structural Roles http://www.iso.org/iso/catalogue_detail.htm?csnumber=63514 |
| [ISO 22600-1] | ISO 22600-1:2014 Privilege Management and Access Control http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62653 |
| [ISO 22600-2] | ISO 22600-2:2014 Privilege Management and Access Control http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62654 |
| [ISO 2382-8] | ISO 2382-8:1998 Information Technology – Vocabulary – Part 8:Security https://www.iso.org/standard/7243.html |
| [ISO 27799] | ISO 27799:2016 Health informatics -- Information security management in health using ISO/IEC 27002 https://www.iso.org/standard/62777.html |
| [ISO 7498-2] | ISO 7498-2:1989 Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture http://www.iso.org/iso/catalogue_detail.htm?csnumber=14256 |
| [ISODE] | Isode Online SPIF White Paper http://www.isode.com/whitepapers/why-spif.html |
| -[ITU X.800] | Security Architecture for Open Systems Interconnection for CCITT Applications; March 22, 1991 http://www.itu.int/rec/T-REC-X.800-199103-I |
| [ITU X.841] | Information Technology - Security Techniques - Security Information Objects for Access Control; 2000 https://www.itu.int/rec/T-REC-X.841/en |
| [Kantara] | https://kantarainitiative.org/ |
| [Kantara Report] | Report from the Blockchain and Smart Contracts Discussion Group to the Kantar Initiative; Thomas Hardjono and Eve Maler; 2017-06-05 https://kantarainitiative.org/file-downloads/report-from-the-blockchain-and-smart-contracts-discussion-group-to-the-kantara-initiative-v1/ |
| [LOINC] | Regenstrief Institute; Logical Observation Identifiers Names and Codes https://loinc.org/ |
| [NIST SP 800-33] | Underlying Technical Models for Information Technology Security http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-33.pdf |

[NIST SP 800-63-3] Electronic Authentication Guideline; 2017
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[NIST SP 800-162] Guide to Attribute Based Access Control (ABAC) Definition and Considerations; 2014
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

[NISTR 8112] National Institute of Standards and Technology Internal Report 8112; Attribute Metadata; Draft August 2016
http://csrc.nist.gov/publications/PubsNISTIRs.html

[NISTIR 8149] National Institute of Standards and Technology Internal Report 8149; Developing Trust Frameworks to Support Identity Federations, Draft Oct 2016
http://csrc.nist.gov/publications/PubsNISTIRs.html

[OIX] Open Identity Exchange, attribute Exchange Trust Framework Specification, Draft Technical Specification V 1.0 , 2 July 2013
http://openidentityexchange.org/wp-content/uploads/2014/06/OIX-AXN-Trust-Framework-Specification-1.0-7-5-2013.pdf

[OMG SEC] Object Management Group; Security Service Specification
ftp://ftp.omg.org/pub/secrtf/15_security_1_5.pdf

[Open XML SPIF] XML SPIF Organization
http://www.xmlspif.org/

[PONDER] The Ponder Policy Specification Language; Nicodemos Damianou, Naranker Dulay, Emil Lupu, Morris Sloman; Department of Computing, Imperial College; January 31, 2001
http://www.doc.ic.ac.uk/~mss/Papers/Ponder-Policy01V5.pdf

[S&I Framework] Standards and Interoperability (S&I) Framework
http://www.siframework.org/

[SNOMED – CT] International Health Terminology Standards Development Organization; Systematized Nomenclature of Medicine – Clinical Terms http://www.ihtsdo.org/

[UMA] User Managed Access (UMA) Profile of OAuth 2.0, v1.0.1
https://docs.kantarainitiative.org/uma/rec-uma-core.html#terminology

[UML] Unified Modeling Language
http://www.uml.org/

[W3C Provenance] W3c Provenance XG Final Report; December 2010
https://www.w3.org/2005/Incubator/prov/XGR-prov-20101214/

[W3C XML] W3C Information and Knowledge Domain
https://www.w3.org/XML/

[WS-Federation] OASIS Web Services – Federation Language (WS-Federation; v1.2, May 2009
http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.pdf

[WS-Trust] OASIS Web Services – Trust (WS-Trust); v1.4, April 2012
http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/errata01/os/ws-trust-1.4-errata01-os-complete.pdf

[XACML] OASIS eXtensible Access Control Markup Language (XACML) 3.0, Jan 2013
http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html



 

[XACML RBAC] OASIS XACML v3.0 Core and Hierarchical Role Based Access Control (RBAC) Profile Version 1.0; October 23, 2014 http://docs.oasis-open.org/xacml/3.0/rbac/v1.0/cs02/xacml-3.0-rbac-v1.0-cs02.pdf

[XSPA] OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) Profile of WS-Trust for Healthcare Version 2.0; July 2013 http://docs.oasis-open.org/xspa/ws-trust-v1.0/xspa-ws-trust-profile-os.pdf


 