V3_PSAF_R1_N3_2019SEP

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

Volume 1: Trust Framework for Federated Authorization Conceptual Model

HL7 Normative Ballot
September 2019

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

IMPORTANT NOTES:
HL7 licenses its standards and select IP free of charge. **If you did not acquire a free license from HL7 for this document,** you are not authorized to access or make any use of it. To obtain a free license, please visit http://www.HL7.org/implement/standards/index.cfm.
If you are the individual that obtained the license for this HL7 Standard, specification or other freely licensed work (in each and every instance "Specified Material"), the following describes the permitted uses of the Material.
A. HL7 INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS, who register and agree to the terms of HL7's license, are authorized, without additional charge, to read, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part without paying license fees to HL7.
INDIVIDUAL, STUDENT AND HEALTH PROFESSIONAL MEMBERS wishing to incorporate additional items of Special Material in whole or part, into products and services, or to enjoy additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS as noted below, must become ORGANIZATIONAL MEMBERS of HL7.
B. HL7 ORGANIZATION MEMBERS, who register and agree to the terms of HL7's License, are authorized, without additional charge, on a perpetual (except as provided for in the full license terms governing the Material), non-exclusive and worldwide basis, the right to (a) download, copy (for internal purposes only) and share this Material with your employees and consultants for study purposes, and (b) utilize the Material for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, Compliant Products, in all cases subject to the conditions set forth in this Agreement and any relevant patent and other intellectual property rights of third parties (which may include members of HL7). No other license, sublicense, or other rights of any kind are granted under this Agreement.
C. NON-MEMBERS, who register and agree to the terms of HL7's IP policy for Specified Material, are authorized, without additional charge, to read and use the Specified Material for evaluating whether to implement, or in implementing, the Specified Material, and to use Specified Material to develop and sell products and services that implement, but do not directly incorporate, the Specified Material in whole or in part.
NON-MEMBERS wishing to incorporate additional items of Specified Material in whole or part, into products and services, or to enjoy the additional authorizations granted to HL7 ORGANIZATIONAL MEMBERS, as noted above, must become ORGANIZATIONAL MEMBERS of HL7.
Please see http://www.HL7.org/legal/ippolicy.cfm for the full license terms governing the Material.

Ownership. Licensee agrees and acknowledges that **HL7 owns** all right, title, and interest, in and to the Materials. Licensee shall **take no action contrary to, or inconsistent with**, the foregoing.

Licensee agrees and acknowledges that HL7 may not own all right, title, and interest, in and to the Materials and that the Materials may contain and/or reference intellectual property owned by third parties ("Third Party IP"). Acceptance of these License Terms does not grant Licensee any rights with respect to Third Party IP. Licensee alone is responsible for identifying and obtaining any necessary licenses or authorizations to utilize Third Party IP in connection with the Materials or otherwise. Any actions, claims or suits brought by a third party resulting from a breach of any Third Party IP right by the Licensee remains the Licensee's liability.

Following is a non-exhaustive list of third-party terminologies that may require a separate license:

Terminology	**Owner/Contact**
Current Procedures Terminology (CPT) code set	American Medical Association https://www.ama-assn.org/practice-management/cpt-licensing
SNOMED CT	SNOMED International http://www.snomed.org/snomed-ct/get-snomed-ct or info@ihtsdo.org
Logical Observation Identifiers Names & Codes (LOINC)	Regenstrief Institute
International Classification of Diseases (ICD) codes	World Health Organization (WHO)
NUCC Health Care Provider Taxonomy code set	American Medical Association. Please see www.nucc.org. AMA licensing contact: 312-464-5022 (AMA IP services)

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

Note to Readers

This document contains the Conceptual Model for the PASS-Access Control Service. The document supports the HL7 Services Aware Enterprise Architecture Framework (SAEAF), under which this project is governed. Further context is given in the overview section below, but one key point to note is that this specification encompasses at the conceptual level, all of the viewpoints identified by the SAEAF.

The Informational Viewpoint section of this document references previous and concomitant work from the Composite Privacy Domain Analysis Model (DSTU) and Security Domain Analysis Model (January 2010 Ballot).

It is critical to note that this specification is NOT the specification of a service, document, or messaging implementation; rather it is an unconstrained conceptual specification of the domain material.

Changes from Previous Versions

The following is a summary of changes from previous versions:

September 2016 - Initial Ballot
V3_PSAF_R1_O1_2016SEP
HL7 Privacy and Security Architecture Framework Release 1
September 2016 HL7 For Comment Ballot
January 2017
V3_PSAF_R1_I1_2017JAN
HL7 Version 3 Standard: Privacy and Security Architecture Framework - Trust Framework for Federated Authorization, Release 1 January 2017 HL7 Informative Ballot
May 2017
V3_PSAF_R2_28_2017MAY HL7 Version 3 Standard: Privacy and Security Architecture Framework – Chapter 2, Volume 1 Trust Framework for Federated Authorization Conceptual Model, Release 2 May 2017 Ballot HL7 Informative Ballot

- Changes required by ballot reconciliation.

V3_PSAF_R2_28_2017MAY HL7 Version 3 Standard: Privacy and Security Architecture Framework – Chapter 2, Volume 2 Trust Framework for Federated Authorization Behavioral Model, Release 1 May 2017 Ballot HL7 Informative Ballot

- Initial Ballot of Behavioral Model

May 2018
May TF4FA includes both (1) a high-level conceptual information model, which represents the privacy, security, and trust policies within each domain that is party to a federated authorization trust contract; and (2) a high-level behavioral model of the services needed to establish such a contract at run-time. In this ballot document, the focal Trust Framework contract is an agreement among policy domains on federated authorization policies.

V3_PSAF_R2_XX_2018MAY HL7 Version 3 Standard: Privacy and Security Architecture Framework – Chapter 2, Volume 1 Trust Framework for Federated Authorization Conceptual Model, Release 2 May 2017 Ballot HL7 Informative Ballot

- Changes required by ballot reconciliation.
- New naming of ballot item –Now Volume 1 with no Chapter number.
- The May 2018 Normative version of TF4FA addresses the ballot comments from the last informative ballot in May 2017 by ensuring alignment with the policy model aspects of ISO/IEC 10181-3 and ISO 22600 needed to establish trust among exchange partners and setting aside consideration of how access control policies are implemented within trust domains. This simplification is intended to create a distinct Trust Conceptual Information and Behavioral Model component within PSAF, which can be coupled with the Privacy Access and Security Services (PASS) Access Control, Audit, and Security Labeling Services Conceptual Models. In time, we expect to update the current normative Composite Security and Privacy Domain Analysis Model to be the overarching PSAF Conceptual Information Model, which will encompass all of the new and revised classes used in the PSAF components.

V3_PSAF_R2_28_2017MAY HL7 Version 3 Standard: Privacy and Security Architecture Framework – Chapter 2, Volume 2 Trust Framework for Federated Authorization Behavioral Model, Release 1 May 2017 Ballot HL7 Informative Ballot

- Changes required by ballot reconciliation.
- New naming of ballot item –Now Volume 2 with no Chapter number.

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 HL7's Trust Framework for Federated Authorization (TF4FA). The documents address core security topics from the perspective of enabling interoperability for information exchange, and include:

- *This 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.
- *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.

The document series illustrates the larger context of establishing trustworthy interoperability for information exchange.

Elements of Trustworthy Interoperability for Information Exchange include:

- Establish Trustworthy Authentication
- Establish Trustworthy Access Control
- Establish Trustworthy Traceability

1 INTRODUCTION

This document describes conceptual-level viewpoints associated with business requirements that relate to the content, structure, and functional behavior of information important to establishing trust in Privacy, Access, and Security domains within the healthcare environment. This document includes the five viewpoints identified by the HL7 Services Aware Enterprise Architecture Framework (SAEAF) at the conceptual level: Enterprise, Functional, Informational, Computational, and Engineering.

This document describes a trust framework approach to federated authorization (TF4FA). The approach involves a high-level harmonized view of trust required to support the interoperability needs of healthcare providers as defined by business relevant use cases (i.e. support security and privacy policies governing protected information exchanged across interoperable Electronic Health Record Systems).[1]

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.

TF4FA allows organizations to dynamically create a Federated Domain wherein participants collaborate in real-time to securely derive necessary access control policy sets and other trust attributes. The result is a mutually-acceptable, common-denominator access policy set that can ensure the proper level of trust, protection, and use of all shared information.

1.1 Overview

TF4FA is a policy-driven approach for controlling access to and use of information across security domains. The policies are derived in real-time by participating domains and agreed to via a computable Trust Contract also established at run-time. This enables an interoperable domain in which an access request for protected information between domains can be processed in accordance with the agreed-upon Trust Contract. Deriving policy generally involves participating domains:

1. Exchanging the set of local access policy applicable to the access request,
2. Identifying differences between those policies, and
3. Using run-time algorithms to iterate with each other as necessary to derive the highest-common-denominator policy set possible.

The TF4FA approach is fully consistent with ISO 22600-2, which states that "co-operation between domains requires the definition of a common set of policies that applies to all of the collaborating domains. It shall be derived from all of the relevant domain-specific policies across all of those domains. These common security and privacy policies are derived through a process known as policy bridging. The eventual agreed policies need to be documented and signed by all of the domain authorities. Ideally, this whole process will be capable of electronic representation

[1] This model can be extended to support the interoperability needs of providers, patients, payers, consumers, researchers, intermediaries, secondary users, app and devices among themselves, and with entities outside of healthcare that involve deriving healthcare-relevant policies.

and negotiation, to permit real-time electronic collaboration to take place within a (pre-agreed) permitted and regulated framework."

1.2 Scope

The scope of this document is the definition of a federated authorization conceptual model for a set of trust services that (a) derive technical and operational rules between domains at run-time, and then (b) create a new interoperability domain (Federated Domain) reflecting those rules. In short, this model focuses on the precursor step of run-time trust derivation of authorization policies and the definition of supporting services.

1.2.1 Out of Scope

The following are out of scope for this document:

- Policy not related to access control decision making.
- Meta Policy and Composite Policy.
- Run-time processing of access requests that use derived policy. This includes access control mechanisms, access schemes, and other access control supporting mechanisms.
- Federated identity, which is about leveraging identity credentials across domains (i.e. cross-domain authentication).[2]
- Modeling a patient-controlled domain.
- Subsequent provisioning of any Trust Contract agreed to by TF4FA participants.
- While identified in the document, the capabilities and semantic information associated with Consent Management and Client Privacy Policy are specifically set out of scope. Subsequent work will be required to elaborate the remaining interfaces.

1.2.2 Preconditions within Scope

TF4FA requires the following pre-conditions for participation:

1. A trust framework for user authentication is already established, mechanisms to establish identity are already done out-of-band, and mechanisms to assert identity across domains are already in place.
2. Mechanisms for secure, trusted exchange of information between participants are already in place.
3. Mechanisms for trustworthy traceability (i.e. audit, data provenance) have been established.
4. Access control policies have been defined within the local participating domains.
5. Patient consent directives are available in the form of privacy policies.
6. TF4FA members meet all legal requirements before disclosing information.
7. TF4FA members use applicable published HL7 standards including HL7 vocabulary, HL7 patient friendly language, and the HL7 Domain Analysis Model.

[2] Though usually dependent upon authentication results, authorization occurs after authentication to determine whether the identified entity has permission to the requested resource.

1.3 Assumptions

This document makes the following assumptions:

- Federated Domain members desire to electronically transact, on their own behalf or on behalf of their users, health information among members.
- Security information exchanged between participants can be verified by reference to sources of authority trusted unconditionally.
- Agreeing to the Trust Contract means that Federated Domain members accept and use the derived results as binding upon participants.
- Federated Domain members agree to use healthcare vocabulary sets, classifications, and security labeling as specified in published HL7 standards.
- Trust contracts are derived (negotiated) such that resource owners do not have to violate any policy of law, regulation, or statute it is bound to uphold with respect to sharing of protected information

1.4 Attributes of a Secure and Trustworthy TF4FA

A trustworthy, secure, scalable federated trust framework maximizes the likelihood of secure information exchange between domains. The characteristics of such a trust framework include:

1. Unique focus on the most difficult and least developed policy area – authorization to collect, access, use, and disclose healthcare information.
2. Enables a "marketplace" of trust relationships rather than a static fiat with no flexibility and no likelihood of alteration without major disruptive changes across the entire ecosystem.
3. Enables interoperation at the highest common denominator via run-time algorithms that use derived access control policy per agreed-upon trust framework contract terms.[3]
4. Enables a flexible "trust fabric" that can involve as many parties who are able to find a mutually-acceptable middle ground for whatever duration and with whatever mix of parties.
5. Provides the capability to make different trust framework "deals" with the same and/or different parties at the same time.
6. Provides a platform-independent information and behavioral model built on foundational ISO security standards as colored by [HL7 DAM].
7. Uses a "federated identity" pattern for run-time derivation of Trust Contracts.

2 ENTERPRISE VIEWPOINT

2.1 Overview

The TF4FA conceptual model identifies the services needed to establish the trust, policy, and information required to implement technological controls for enforcing healthcare security and privacy policy within a federated authorization trust framework.[4]
Identified within the Enterprise Viewpoint are the business issues, models, processes, and roles associated with the Trust Framework sub-domain of Privacy, Access, and Security Services.

2.1.1 General Policy Model

The concepts of the control model as identified in [ISO TS 22600], Privilege Management and Access Control – Part 2: Formal Models are extended in this document. We adopt 22600 models including meta data and composite policy.

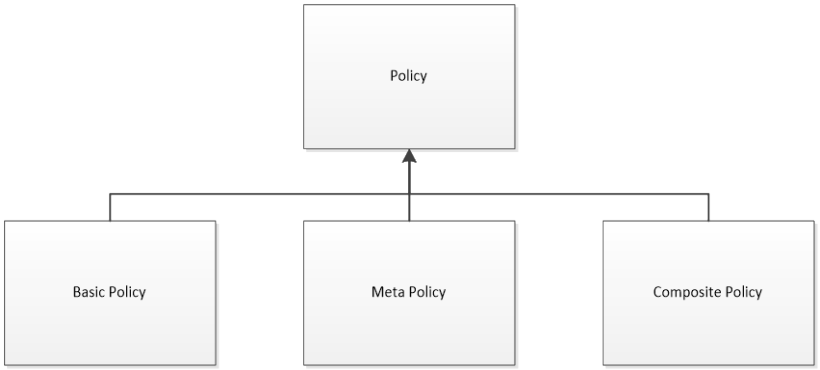

Figure 1: General Policy Model

To be able to exchange information among security domains, there must be an agreed set of security policy rules for this exchange. These security policy rules are called secure interaction rules. They are part of each security domain's security policy rules where both the semantics and the representation of the security information are different in each of the security domains. Secure interaction rules must specify how security information of one domain is to be translated into security information of the other domain. Syntax translation may also be necessary. [ISO 10181-1]

2.1.2 Trust Contract Model (Execute Contract)

Federated authorization 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 contracts are derived by Trust Framework Services, each of which derives a specific aspect of the Trust Contract or service. Throughout, attributes pertain to those required for authorization purposes.

During the Trust Contract Phase, Federated Domain members sign a computable Trust Contract, and thus agree to be bound by the common policies established for trustworthy exchange. This phase requires successful completion of the Policy Derivation Phase.

[4] Security is the mechanism for enforcing privacy policy.

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 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 privacy policies that apply equally to all members. Trust Contracts can have a time limit, whereupon a new, complete Trust Contract must be established.

Figure 2 summarizes the relationship between a Trust Contract and its environment. The dotted grey arrows indicate that the Trust services establish the Trust Contract, and the Policy Information Model helps establish the Federated Policy.

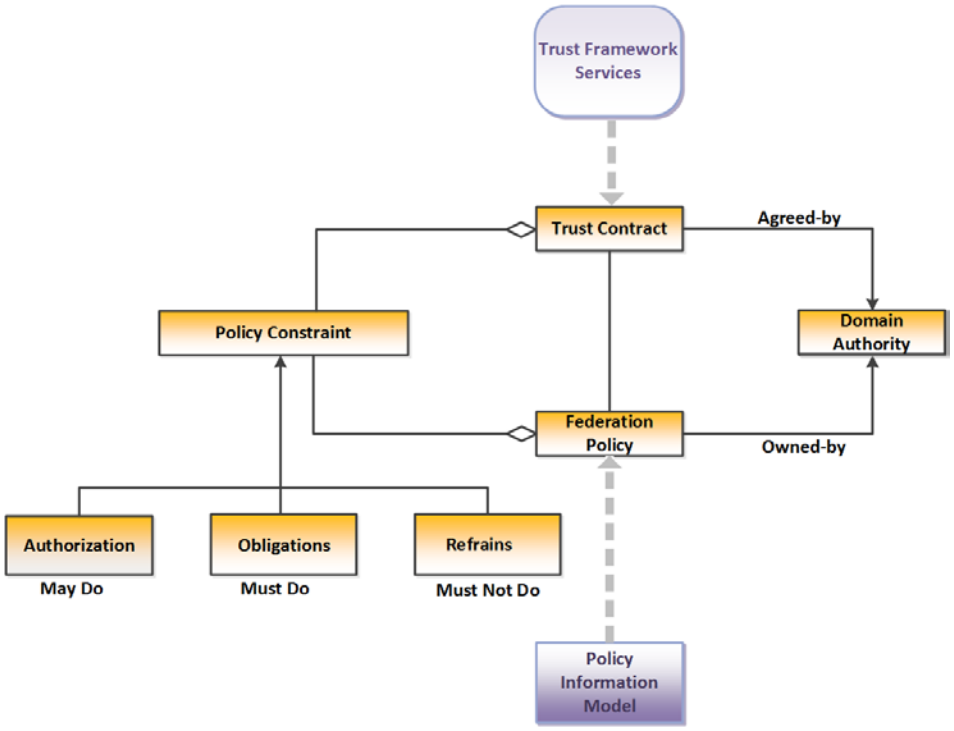

Figure 2: Relationship of a Trust Contract to its Environment

This phase may include manual intervention by relevant member stakeholders to review and approve the Trust Contract.

Trust Contracts are peer-to-peer, instance-based contracts between members. The members determine whether a Trust Contract does or does not persist beyond the current transaction.

2.1.3 Trust Policy Governance Model

Within the scope of the Trust Framework model, a Federated Domain means any domain operating under policies of trust, within a trust context, such that one member may make requests for, and then receive protected information from another. Within this contextual framework, a security and privacy policy exists constrained by jurisdictional, organizational and subject of care policies. The Trust Context includes the entire complex of legal, ethical, social, organizational,

psychological, functional, and technical rules for ensuring trustworthiness of health information systems. [ISO 22600-2].

A 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. Generally, an entity can be said to "trust" a second entity when it (the first entity) makes the assumption that the second entity will behave exactly as the first entity expects. [ISO 22600-2]

TF4FA results in a Federated Domain, which operates under access control policies of trust such that one member may make requests for and then receive protected information from another. Figure 3 illustrates, the access control policies of trust are security and privacy policies that exist within a contextual framework constrained by jurisdictional, organizational, and subject of care access control policies. The overall trust context includes environmental, legal, social, and technical components.

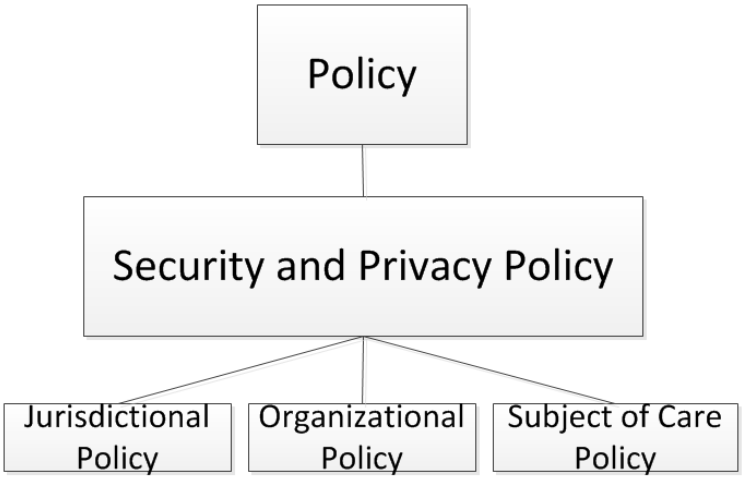

Figure 3: Policy Governance Model

The TF4FA model reuses security standards across the enterprise to enforce access control policies required by:

- **Jurisdictional Policy** – Class of policy used to represent a territorial authority that may be issuing privacy and/or security policies for a territory
- **Organizational Policy** – Class of policy used to represent an organization that may be issuing privacy and/or security policies.
- **Subject of Care Policy** – Privacy policies in the form of individual patient consent directives.

Trust negotiation occurs as a distinct pre-cursor activity prior to the instantiation of any specific run-time request. Trust negotiation establishes the operational context for requests for information.

At run-time, access control mechanisms enforce disclosure of protected information from the resource domain to the initiator domain based upon access control schemes. Requests for information are made and adjudicated. If successful (i.e. access request approved), protected information may be exchanged from one party to another for use as specified within a computable contract of trust.

Adjudication involves an access control mechanism, which 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 [ISO 10181-3]. Examples of access control schemes include role-based access control (RBAC), attribute-based access control (ABAC), access control lists (ACLs), and relationship-based access control (ReBac).

In summary, a Federated Domain is a domain operating under policies of trust such that one domain user may make requests for, and then receive protected information from another domain member. The Federated Domain has the following characteristics:

1. If both parties accept and mutually agree to bind themselves to the policies of exchange, then a contract of trust may be established.
2. Federated resource domains disclose protected information if initiators assert conformance to the trust contract.
3. Initiators have authority to make requests for information from Federated Domains with which they are affiliated.
4. At runtime, initiators must prove who they are and assert request-bound access control decision information (ACI) acceptable to resource domain access control services.

2.1.4 Generalized Trust Service Model

Figure 4 shows the generalized trust model (adapted from [ISO 22600-2]) upon which TF4FA is based. A service requester (sometimes called initiator or user) submits a trust proposal to service provider (sometimes called target or resource). The trust proposal specifies a list of users on the requesting side that would like access to a list of information resources hosted by the provider for a stated duration in accordance with a particular trust contract.

See Table (or Glossary) for terminology equivalency between standards

The Figure below is a representation of trust derived from [ISO 22600-2].

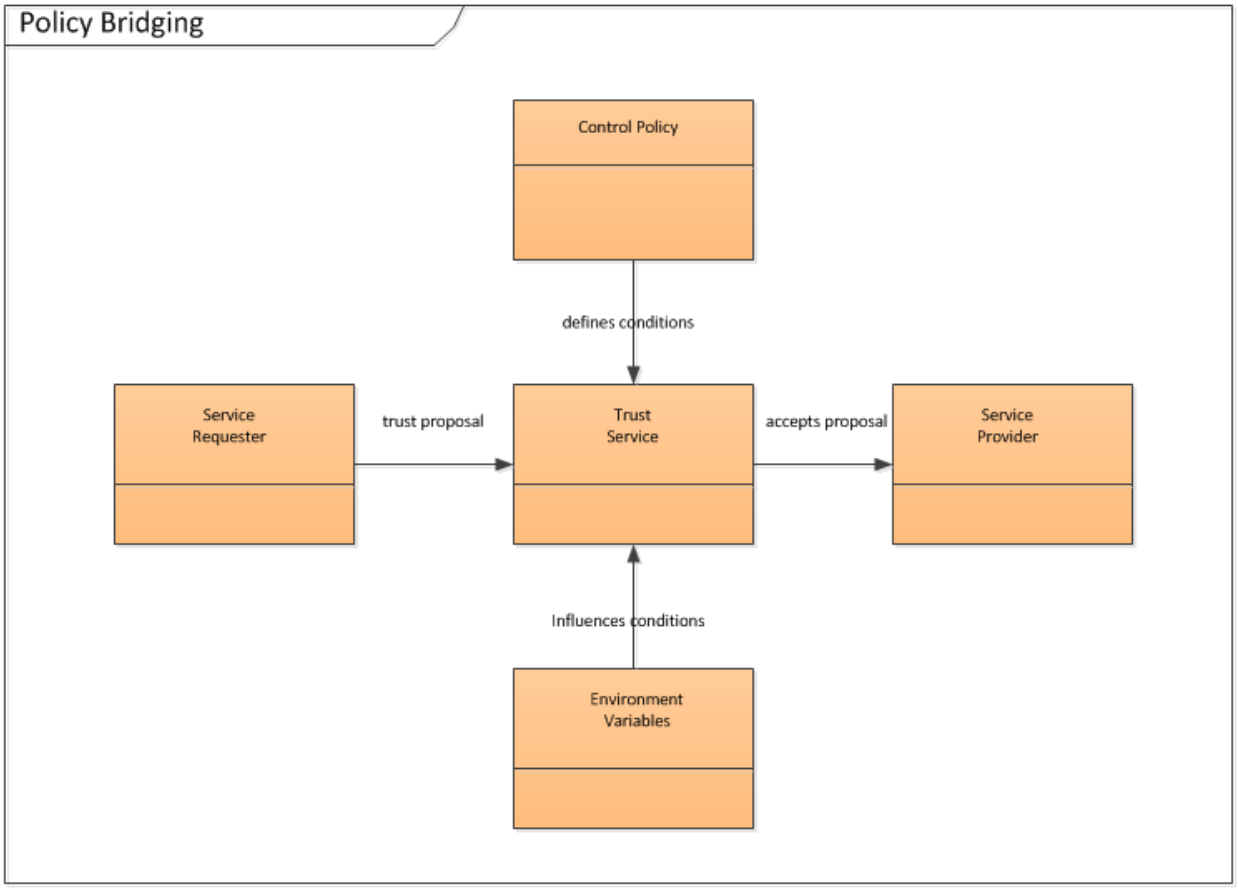

Figure 4: Generalized Trust Service Model

The parties use trust services to attempt to derive a common set of security and privacy policies for use in information exchanges relating to the offered trust proposal. This is the policy bridging process. Examples of derived policy include:

- Just the service provider's access policy. This supports one-way information exchange.
- The access policy of both the service requester and service provider. This supports two-directional information exchange.
- A single access policy if the service requester and service provider sides have the exact same policy. This supports both one-way and two-way information exchange.

Requester and provider access control policies as well as environment variables are key inputs. Access control policies, reflective of the information model, define the conditions (rules) for access. Environment variables (e.g. date, time, location) influence the conditions of access.

Ultimately, the service provider must accept the trust proposal, and all parties must agree to the derived policy for trust to be established and subsequent information exchange to be performed.

The Service Requestor has certain privilege attributes provided by an authority that is trusted by the Access Control Service. The Service Provider is a protected resource with certain attributes that influence the selection of an appropriate Policy or the path through the policy that

is applied to the proposal. Environment variables may provide additional factors that may impact evaluation of the policy.

When a trust proposal is accepted, both parties acknowledge the conditions by executing and asserting adherence to conditions of a trust contract negotiated by the Trust Service. Thereafter, the Access Control Service protects the Service Provider from unauthorized access in accordance with the Control Policy.

2.1.5 Federated Trust Reference Model

Figure 5, below shows an expanded view of the Federated Trust Reference Model, exposing trust in the context of generalized access control policy types (per ISO), associated Domain elements and Trust Service activities. Consistent with PASS ACS, the model is a general one, and applies to any number of verticals/industries and is in itself not healthcare specific. In particular, there is no component that is explicitly limited to a healthcare environment. The possibility for healthcare specific concerns exists only in the Domain and Policy definitions.

The Federated Trust Reference Model describes the components of negotiated trust between two or more individual domains that provide a basis for assuring secure interchange of protected health information. Exchange occurs under the control of shared security and privacy policies managed by a common Federation Authority. The shared domain of data, users, and policy defines the elements of a resulting Federated Domain.

As discussed above, trust negotiation occurs independently of any specific information request. Therefore, trust and trust contracts are not concerned with the details of individual information requests such as the actual values of runtime access control decision information. The Trust Framework model intends to produce a contract governing all related requests. As a consequence, the Trust Framework is principally concerned with aspects of Basic Policy, while Meta-Policy and Composite Policy are additional external aspects needed to support run-time operation of a functioning Access Control service.

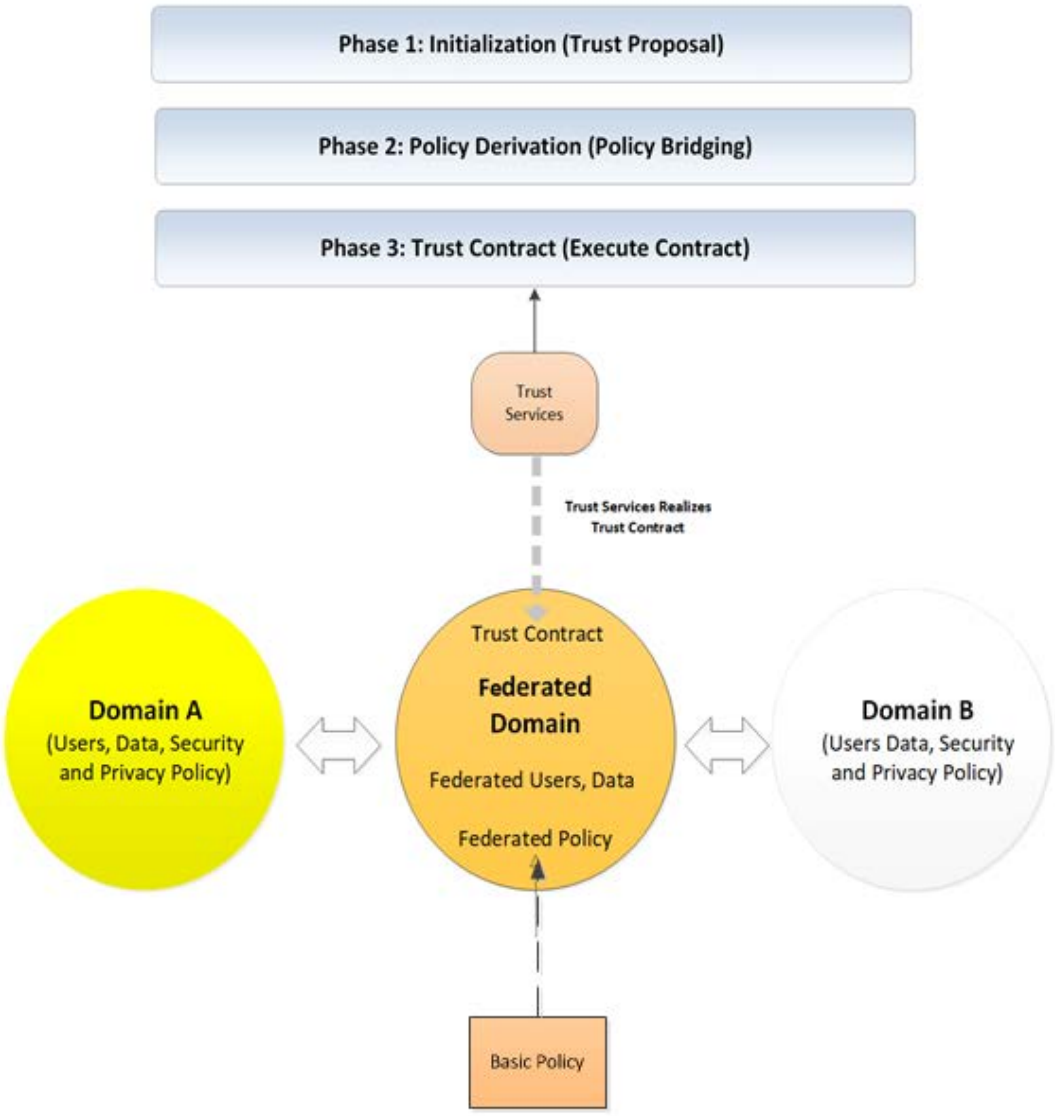

Figure 5: Federated Trust Reference Model

Figure 6 shows the result of a system where policy bridging has derived the set of common, domain-specific security and privacy policies required for trustworthy co-operation between collaborating domains (Federated Domain Composite Policy). Derived from [ISO].

According to Figure 6 TF4FA encompasses three constituent models, each of which is dedicated to defining an essential element of the overall TF4FA:

- **Trust Services Model** – describes the services that derive and codify trust and access control policy at run-time between domains participating in a cross-domain access request transaction.
- **Federated Domain Model** – describes the interoperable domain that results from two independent domains deriving trust and access control policies.
- **Policy Class Model** – describes the policy information model needed to make a proper access request and use decision.

The constituent models work closely with each other. The Trust Services Model enables policy bridging of the healthcare information model defined in the Policy Class Model to harmonize TF4FA participants' access control policies. It also creates a computable trust contract that binds the participants to harmonized policy. The harmonized policy, manifested in a trust contract, underpin the Federated Domain defined in the Federated Domain Model.

The phases of Trust Service facilitate establishment of an agreed-upon Trust Contract and Federated Policy. The Federated Domain is an interoperability domain for participants to share protected information between them in accordance with the agreed-upon Trust Contract and Federated Policy. It also shows that only selected users and resources are included in the Federation Authorization Domain as necessary for the specific business reason for establishing the Federated Domain in the first place.

The Policy Class Model is the basis of Federated Policy used within the Federated Domain.

This model is purely conceptual. Nothing in this model is intended to be a technical specification or a technical design. In addition, this model is technology and platform independent

Descriptions of abstract capabilities of this model are provided throughout the document; they should not be viewed as concrete concepts or requirements.

The TF4FA model identifies the services needed to establish the trust, policy, and information required to implement technological controls for enforcing healthcare security and privacy policy within a federated authorization trust framework.[5] In doing so, the model focuses on security policy and privacy policy and shows the relationship between them.

2.2 Establishing Trust

Establishing trust necessary to permit information exchange within a Federated Domain requires phased coordination among participants. Some exchange phases, and some activities within phases, may be done in any order deemed necessary or in parallel. Some phase portions may be iterative, requiring back and forth between participants until agreement is reached or a decision to stop trying is made. Regardless of the sequencing participants choose to use, all elements of trust that allow information exchange between disparate systems must be derived and mutually agreed to prior to requests and disclosure of protected information.

The Federated Domain model describes the components of negotiated trust between two or more individual domains that provide a basis for assuring secure interchange of protected health information. Exchange occurs under the control of shared security and privacy policies managed by a common Federation Authority. The shared composition of data, users and policy defines the elements of the Federated Domain

Domain Authorities agree to which users and what data are to make up the shared Federated Domain, and the rules governing information sharing. A Trust Contract (also called Federation Agreement) provides confidence that the mutual agreements will be honored by recording the following:

- The rights given to both sides, such as the kind of access allowed
- The trust each has in the other
- An agreement as to how policy differences are handled, for example, the mapping of roles in one domain to roles in another

[5] Security is the mechanism for enforcing privacy policy.

In a federation, each domain retains most of its authority while agreeing to afford the other limited rights.

Under domain rules, data sensitivity is computed as the maximum level and a domain may only contain single data sensitivity - this is called Sensitivity[6] Singularity. However, to achieve real-world conditions, the full description of all desired interactions among cooperating partners involves the chaining together of multiple individual federated subdomains representing all included sensitivities. The resulting extended domain forms a federated multi-domain of communication and cooperation characterized by mutually agreed upon overall security and privacy policies.

1. In a Federated Domain, Initiators have authority to make requests for information from Resources.
2. If both parties accept and mutually agree to bind themselves to the policies of exchange, then a Trust Contract may be established.
3. Resources disclose protected information if Initiators assert attributes conforming to trust policy.
4. At request run-time, initiators must prove who they are and assert request-bound access control decision information (ADI) acceptable to the Resource.

In a Federated Domain, requests for information are made and adjudicated. If successful, protected information may be exchanged from one party to another for use as specified within a Trust Contract. Information exchange occurs following successful execution of the following steps:

Trust Contract Phase (Execute Contract)

During the Trust Contract Phase, Federated Domain members sign a computable Trust Contract, and thereby agree to be bound by the common policies established for trustworthy exchange. This phase requires successful completion of the Policy Derivation Phase.

This phase may include manual intervention by relevant member stakeholders to review and approve the Trust Contract.

Trust Contracts are peer-to-peer, instance-based contracts between members. The members determine whether a Trust Contract does or does not persist beyond the current transaction.

[6] "Sensitivity" refers to the confidentiality classification of the data as defined in [HL7 HCS]: "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. 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."

Table 1: Trust Framework Service Capability

HL7 PASS ACS Trust Framework Service Capability	Supplemental Guidance	Where Addressed by TF4FA
Establish Legal Framework Between Domains	The objective is to describe the actual legal framework including rules and regulations, responsibilities, and liabilities. A legal framework must be agreed upon for acknowledgement to occur.	Policy Derivation Phase. See Trustworthy Authentication volume for more details. Trust Contract Phase.
Coordinate Authentications Across Domains	Authentication of users/roles should be based on PKI according to ISO 17090. When different methods are used by participating domains, an approach should be agreed upon by all participating domains and specified in a federated domain policy. [7]For cases where the participating domains cannot agree upon a common standardized authentication system, ISO 22600 specifies a number of stipulations to be met.	Policy Derivation Phase. See Trustworthy Authentication volume for more details. Trust Contract Phase.
Define Identity Verification & Linking Methods	The federated domain policy defines the identity validation and/or verification methods used in the domains, including identity proofing for methods used in the security and privacy policy domains for the identification of principals such as persons (patients, healthcare professionals, health professionals, etc.), organizations, systems, devices, applications, components, etc. If different identification systems are used, the applied system has to be defined. Linking, mapping, or conversion mechanisms need to also be defined. In that context, the use of a unique patient ID as well as namespace-related master patient indexes and the use of a patient identification service should be considered and specified.	Policy Derivation Phase. See Trustworthy Authentication volume for more details. Trust Contract Phase. Additional types of matching (e.g. object identifier matching) may be performed as necessary.
Harmonize Access Privileges Across Domains	Rules for access privileges are agreed upon by participating domains and specified in the federated domain policy. The circumstances allowing access to the information in another domain are described in ISO 22600-2.	Initialization Phase. Policy Derivation Phase. Trust Contract Phase.

[7]

HL7 PASS ACS Trust Framework Service Capability	Supplemental Guidance	Where Addressed by TF4FA
Harmonize Rules for Patient Consent	The rules for patient consent have to be harmonized. If harmonization is not possible, principles have to be defined ruling how differences shall be bridged. The rules for patient consent are agreed upon by all participating domains and specified in a federated domain policy.	Initialization Phase. Policy Derivation Phase. Trust Contract Phase.
Define Data Integrity Methods & Rules When Transferring Data	The methods and rules for checking the integrity of data shall be defined in order to detect unauthorized modification of data during transfer between the participating domains. The rules and techniques for such integrity check are agreed upon by all participating domains and specified in a federated domain policy.	However, Policy Derivation Phase allows participants to indirectly agree on a data integrity approach (e.g. via asserted Data Use Agreement or Trust Framework participation) Also Addressed in Trustworthy Traceability volume.
Ensure Patient Privacy Rules are Clear to Patients	Patient privacy is a key issue in communication across policy domain boundaries, and especially in trans-border information exchange. In order to gain a patient's full confidence with the information transactions, it is of utmost importance that the rules are clear and easily understood by the patients. The rules and techniques for ensuring clarity of patient privacy rules are agreed upon by all participating domains and specified in a federated domain policy.	HL7 TF4FA requires use of HL7 standard vocabulary / code sets and patient friendly language.
Harmonize / Map Security and Privacy Policies Across Domains	Security and privacy policy domains are distinguished by their policies. Ideally, the communicating and cooperating security and privacy domains can commit to one and the same security model represented by a harmonized policy. This is the primary goal, and the security standards defined at ISO (See Volume 1, Appendix C under 'reference standards') are the primary tools for achieving this. If such harmonization is not possible, the domain policy specifies which policy can be considered equivalent for which role, information, action, and purpose. For each role, information, action, and purpose, a set of policies has to be defined. In cases where	Initialization Phase. Policy Derivation Phase. Trust Contract Phase.

HL7 PASS ACS Trust Framework Service Capability	Supplemental Guidance	Where Addressed by TF4FA
	policies cannot be processed by the systems involved, security levels have to be defined including the related rules and the equivalences between them. See also ISO 22600-2	
Define Procedures to Access Data Across Domains	The domain policy defines the procedure of accessing data across participating domain boundaries. For different access modes such as read-only, transfer, process, or communicate, accessible information might be different. Therefore, information needs to be identifiable at the granularity level needed.	Overall TF4FA model that defines a Trust Contract that controls exchange of information.
Define Authorization Process	The authorization process is defined in the domain policy both internally to the security and privacy policy domain and between the interconnected domains.	Overall TF4FA model that defines the Trust Contract that controls exchange of information.
Define Method to Specify Cross-domain Data Location/Structure	In order to secure the information retrieval, location and data structure of applications have to be specified and understood by all parties. The domain policy contains detailed information about the location and structure of data, uniquely described by identifiers such as URLs and/or object identifiers (OIDs).	Policy Derivation Phase. See Trustworthy Authentication volume for details.
Harmonize / Map Role Structures Across Domains	Roles are defined within each security and privacy policy domain. Privileges as well as contextual and environmental conditions are defined in policies that are bound to one or more roles. Role assignments and assertions are essential parts of the solution for the final policy bridging.	Initialization Phase. Policy Derivation Phase. See Trustworthy Authentication volume for details. Trust Contract Phase.

As the Trust Services Model and Policy Class Models illustrate above, they are bridged by a Federated Domain Model.

As further depicted by the diagrams above, a domain is a set of active entities (person, process, or device), their data objects, and a common security policy. [NIST SP 800-33]. Individual domains (local domains) can be combined to create a composite domain called a Federated Domain. The join of these sub-domains and their intersections joining shared users, data, and policy are established via a joint consolidated policy manifested in a Trust Contract agreed to by the domain authorities. As a result, within a Federated Domain, users are able (based upon their authenticated identities and authorizations) to access information objects at a given sensitivity level according to a distinct, applicable access control policy

The common security policies are assumed to operate under jurisdiction of one or more domain authorities. Additional domain attributes include:

- Within a security domain, all information objects exist at the same level of sensitivity [ASTM E2595]. Note: this is synonymous with the "confidentiality classification" found in HL7 HCS.
- Members of a domain may have different security attributes, such as read, write, or execute permissions on information objects. [ASTM E2595]
- Security domains are not bound by systems or networks of systems. [ASTM E2595]
- A security domain's objects may reside in multiple systems. [ASTM E2595]

Where definition of shared users, data, and policy cannot be determined, then a federated sub-domain domain or even domain cannot be defined and by definition interoperability between domains or particular sub-domains may not be possible.

2.2.1 Initialization Phase (Present Trust Proposal)

Federated Trust is derived (negotiated) between domains and manifested in computable Trust Contracts. Negotiation begins with the initiation of a Trust Proposal, which may be included in a request for information along with trust assertions of identity. During the negotiation participants propose trust elements relevant to the exchange. Negotiation may involve multiple proposal/counter-proposal iterations before finally reaching a mutually agreed upon set of Federated Policies (Contract) that can be used to control information requests.

During the Initialization Phase, policy context is established by one domain presenting an initializing trust proposal to another domain. The trust proposal is manifested as "my [list of] users request access to [a list of] your information while the provisions of my proposed trust contract are in effect."

Defining users may be as specific or general as required, for example, Dr. Bob, all persons with a specific role (e.g. Oncologist, Dentist, or Licensed Healthcare Provider, etc.). User in this case means Initiator Domain User(s), which can be an Organization, person, device, process, or system.

Similarly, domain information may also be specific or general (e.g. a single Blood Pressure reading, a specific patients' entire Medical Record, or patient information for all patients with a specific condition, etc.)

- Establish trust in the identity of Initiator Organization/User(s)
- Establish trust in the identity of the Target
- Establish structural aspects of the exchange (e.g. message format standards)
- Establish semantic aspects of the exchange (e.g. codification, vocabulary, and standards to apply so that the receiving system can interpret the data)
- Establish the run-time aspects of the exchange including defining environmental or request related information.

2.2.2 Policy Derivation Phase (Policy Bridging)

During the Policy Derivation Phase, policy context is established via policy bridging. Context includes the legal, political, organizational, functional and technical obligations aspects that are to apply to the exchange, including leveraging understood and existing foundations. Bridging also includes the technical frameworks used for information exchange, authorization, terminology (i.e. value sets), and data use agreements. Examples of activities that may take place during policy bridging are:

- Establish the legal aspects of the exchange (e.g. the governing security and privacy jurisdictional, organizational laws, rules, and regulations)
- Establish patient choice aspects of the exchange
- Establish location of pre-existing trust criteria, qualifications, licenses, third-party attestations, certifications and/or trustmarks.

Policies may be exchanged directly between domains and from public-facing external policy management services.

Establish Trust Contract Phase (Trust Contract)

Contracts are derived by Trust Framework Services. Agreement to abide by the conditions of trust is manifested in a computable Trust Contract, a machine- derived (negotiated) signed agreement binding upon participants. Once signed, Trust Contracts establish the legally binding business and technical operational rules among Federated Domain members

To achieve agreement, it may be necessary for the Initiator to modify their original Trust Proposal/Request for Information to conform to the access policy requirements of the Target. In negotiation, the acceptance of the data owner is the primary objective with the principle that data owners would not be required to exchange protected information in manners inconsistent with their own governing policies. If participants cannot agree on a Federated Policy, information exchange may not be possible.

2.3 Trust Scenario Development

During our business analysis, we examined a number of healthcare-specific scenarios that lay the foundation for describing the interactions upon which the use cases are based. The scenarios below expose some specific semantic or behavioral aspect of the process of establishing a Trust Framework in a healthcare environment from creating an initial trust proposal for interoperable exchange to a decision to accept, reject, or counter a proposal, through the policy bridging process to develop a counter proposal, and the decisions as to whether to continue negotiations or to stop the process.

Given that SAEAF is based on RM-ODP, MDA, and the RIM, the TF4FA scenarios follow the RIM modeling methodology using Interaction diagrams to capture the events in a process sequentially at a high level and to depict these events as storyboards to set the real-world context from which the business requirements were derived.

- **Storyboard.** A means of providing context to the definitions of trigger events.
- **Storyboarding Process.** The process of storyboarding lays the foundation for describing HL7 messages and their content.
- **Purpose.** The purpose is a short narrative that describes the generic set of actions that the storyboard represents.
- **Events.** A storyboard narrative is a description of a real-life event that provides the necessary context for the development of a specific interaction described in the storyboard.
- **Actors.** The names of persons, places and organizations that are used in storyboards and examples are fictional
- **Storyboard Interaction Diagram.** The Storyboard Interaction Diagram shows the interactions between the application roles. These interactions are typically depicted using a sequence diagram.

2.3.1 Overarching Storyboard

Figure 6 Trust Framework Interaction Diagram shows the interactions between Trust Framework roles (Trust Services) supporting the exchange of trust information leading to the establishment of a common agreement (Trust Contract) preliminary to the exchange of protected information.

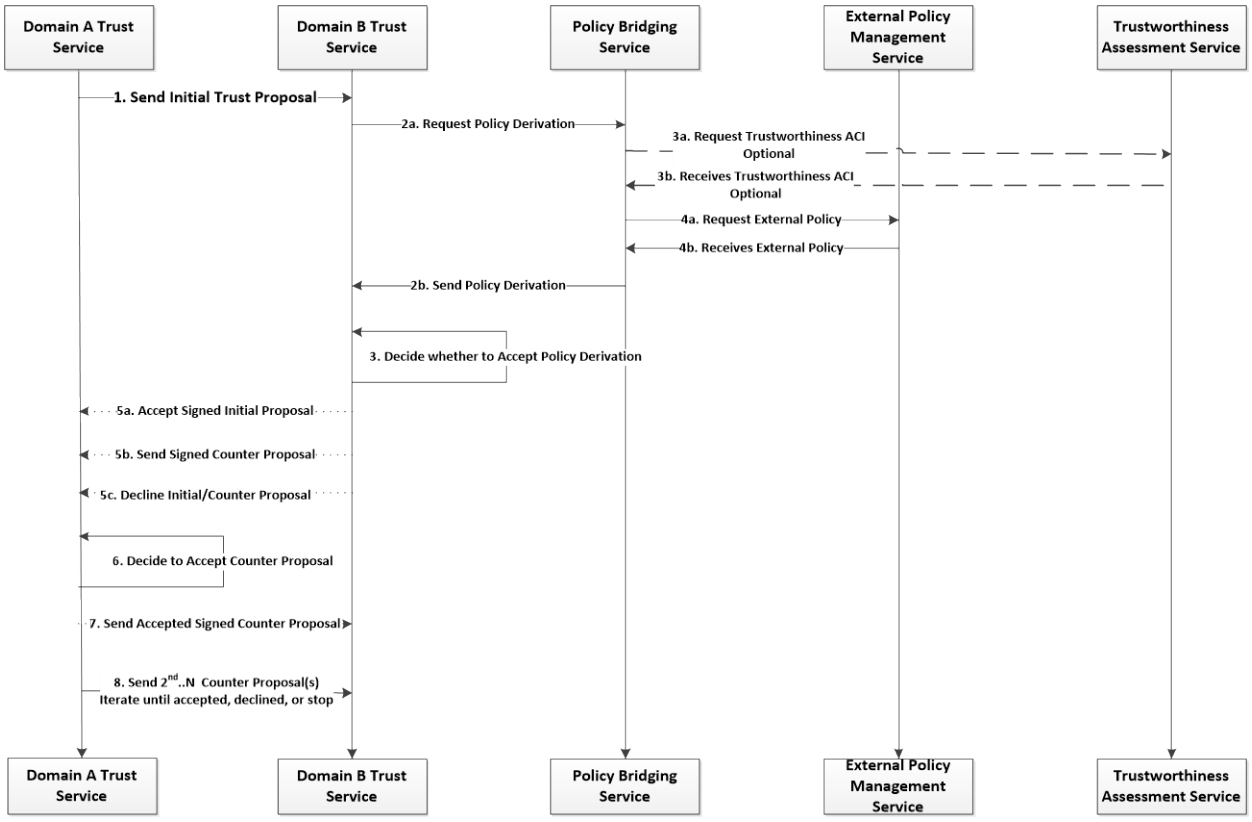

Figure 6: Trust Framework Interaction Diagram

Description

HIE A has small Primary Care Provider PCP clinics on the border of HIE B state lines. HIE A PCPs send patients to HIE B state for specialty, outpatient, and inpatient care, especially for conditions which are related to specially protected information (SPI) because the nearest HIE A state facilities are substantially distanced from HIE PCP clinics

HIE A PCP clinic need HL7 Version 2 Admit, Discharge, and Transfer message notifications (ADT) from HIE B to inform PCP clinics about out of state care provided to their patients.

HIE B participants are required under HIE B's governance contract to apply security labels with the privacy tags at the message segment header level of all ADTs for the high-water mark (most restrictive of any content level security labels), and at specific segments that contain SPI. This enables HIE B participants to share health information governed under HIPAA and SPI related information as authorized by the HIE B patient consent directives, i.e. providers authorized to access SPI are able to access, collect, and use both HIPAA and SPI related information, while providers not authorized for SPI are able to access, collect, and use HIPAA governed information.

HIE A participants are not required to apply security labels at the content level, only at the header level. As a result, only HIE participants authorized to access, collect, or use SPI are authorized to receive ADTs that include SPI.

Nevertheless, HIE A wants to facilitate interoperable exchange of SPI from HIE B to authorized HIE A participants, in particular, HIE A's PCP clinics, which are referring patients with SPI conditions across state lines to HIE B.

To do so, HIE A must create a Trust Proposal to HIE B, which stipulates provisions in keeping with its capability to disclose SPI ADTs to authorized HIE A participants. The following storyboards describe the events and actors involved, and the events in the process by which HIE A's Trust Proposal is processed between HIE A and HIE B.

2.3.2 Trust Initial/Modified Trust Proposal Scenario (1)

Storyboard description

HIE A sends a Trust Proposal to receive SPI ADTs from HIE B, and to disclose to authorized recipients in compliance with HIE B SPI patient consent directives, based on ADT message header segment security labels.

Actor(s)

HIE A Trust Service

HIE B Trust Service

Trigger Event

Create new or modified trust proposal.

Map to Use Case – TF-1 Create Trust Proposal Description:

- Domain A has a set of users that require access to healthcare information owned by Domain B, or
- Use Case TF-7: Review Trust Counter Proposal returns a result indicating a need to modify the original request in order to be able to meet Domain B's data sharing requirements.

2.3.3 Request Policy Derivation 2a

Storyboard description

HIE B reviews HIE A Trust Proposal to share SPI ADTs with security labels only at the header level. HIE B Trust Service requests that its Policy Derivation Service resolve this policy request.

Actors

HIE B Trust Service

Policy Derivation Service

Trigger Event

HIE A Receives Trust Proposal from HIE B

Maps to Use Case TF-2: Review Trust Proposal Description

The trust proposal is reviewed for completeness and compliance with Domain B's data sharing requirements. This review may trigger the involvement of additional services in order to gather completeness and compliance information.

2.3.4 Send Policy Derivation Results Scenario 2b.

Storyboard description

Policy Derivation service sends HIE B the results of comparing HIE B policies retrieved from the External Policy Management Service for disclosing SPI labeled at a granular level with HIE A trust proposal to receive SPI labeled at the header level. Derivation results are that HIE B can share SPI at the header level with HIE A if HIE A agrees to only disclose ADTs per header level security labels to participants authorized to receive SPI. Resulting policy is that HIE A must not disclose SPI ADTs to any participant not authorized to receive SPI, and that authorized end users must comply with limitations on purpose of use, minimum necessary use, and no re-disclosure without consent per SPI patient privacy consent directive.

Actors

Policy Bridging Service

External Policy Management Service

HIE B Trust Service

Trigger Event

Complete Policy Derivation

Map to Use Case TF-2 Review Trust Proposal

Derive (negotiate) the set of common, domain-specific security and privacy policies required for trustworthy co-operation between collaborating domains.

2.3.5 Request Trustworthiness Assessment Scenario 3a (Optional)

Storyboard description

HIE B consults a Trustworthiness Assessment Service to assess current HIE A's reliability, reputation, relationships among other metrics, and disclosure activity patterns, for indications of run-time trustworthiness confidence.

Actors

Policy Bridging Service

Trustworthiness Assessment Service

Trigger Event

Receive Policy Derivation Request

Maps to Use Case TF-4: Assess Partner Trustworthiness

2.3.6 Receive Trustworthiness Assessment Scenario 3b (Optional)

Storyboard description

HIE B receives results of the Trustworthiness Assessment.

- Happy Path – Results of the Trustworthiness Assessment comply with HIE B's policies, so HIE B proceeds with the negotiation of a trust contract, or
- Unhappy Path - Results of the Trustworthiness Assessment do not comply with HIE B's policies. HIE B may consider escalating trust verification or decline to proceed with negotiations of a trust contract.

Actors

Request Trustworthiness Assessment Service
Policy Bridging Service

Trigger Event

Complete Trustworthiness Assessment

Maps to Use Case TF-4: Assess Partner Trustworthiness

2.3.7 Request External Policy Scenario 4a

Storyboard description

HIE B Policy Bridging Service requests HIE B relevant trust policies and contracts from an External Policy Management Service.

Actors

Policy Bridging Service
External Policy Management Service

Trigger Event

Request External Policy (2a)

Map to Use Case TF-5: Discover External Policy

TF-5 Pre-Condition: The Policy Bridging Service determines a need for additional policy information not contained in the original trust proposal.

2.3.8 Receive External Policy Scenario 4b

Storyboard description

HIE B Policy Bridging Service retrieves HIE B relevant trust policies and contracts from an External Policy Management Service.

Actors

External Policy Management Service
Policy Bridging Service

Trigger Event

Receive External Policy (4b)

Map to Use Case TF-5: Discover External Policy

TF-5 Post-Condition: Policy and compliance information is returned to the Policy Bridging Service

2.3.9 Accept Signed Initial Proposal Scenario 5a

Storyboard description

HIE B accepts and digitally signs the initial proposal from HIE A after its Policy Derivation Service resolves HIE A policy request finding it in conformance with HIE B standing trust policy for disclosing SPI to HIEs with the capability of access control at the header level.

Actors

Domain B Trust Service

Domain A Trust Service

Trigger Event

Decide whether to Accept Policy Derivation (3)

Map to Use Case TF-2: Review Trust Proposal

2.3.10 Send Signed Counter Proposal Scenario 5b

Storyboard description

HIE B sends a signed counter proposal based on results of its Policy Derivation Service. For example, if HIE A requested that SPI ADT be sent to payers, HIE B Policy Derivation Service may return the policy bridging result that sending treatment information in ADTs to payers does not comply with HIPAA treatment purpose of use and recommend that HIE B either decline HIE A trust proposal or counter with a proposal limiting the authorized users to providers for purpose of use treatment.

Actors

Domain B Trust Service

Domain A Trust Service

Trigger Event

Decide whether to Accept Policy Derivation (3)

Maps to Use Case TF-2: Review Trust Proposal

2.3.11 Decline Initial/Counter Proposal Scenario 5c

Storyboard description

HIE B declines HIE A trust proposal to receive HIE B ADTs for purpose of use population health and research purpose of use because these purposes of use for ADT are not permitted under HIE B governance.

Actors

Domain B Trust Service

Domain A Trust Service

Trigger Event

Decide whether to Accept Policy Derivation (3)

Maps to Use Case TF-2: Review Trust Proposal

TF-2 Post-Conditions:

All policy and compliance information is received and used to determine if the trust proposal is either:

- Acceptable as submitted (i.e. doesn't require a counter proposal).
- Not acceptable as submitted and therefore:
  - Requires a counter proposal in order to exchange information, or
  - Policy and compliance information returned triggers a termination of the transaction.

2.4 Use Cases

The boundary diagrams below illustrate the relationships among Access Control Services and Trust Management Services.

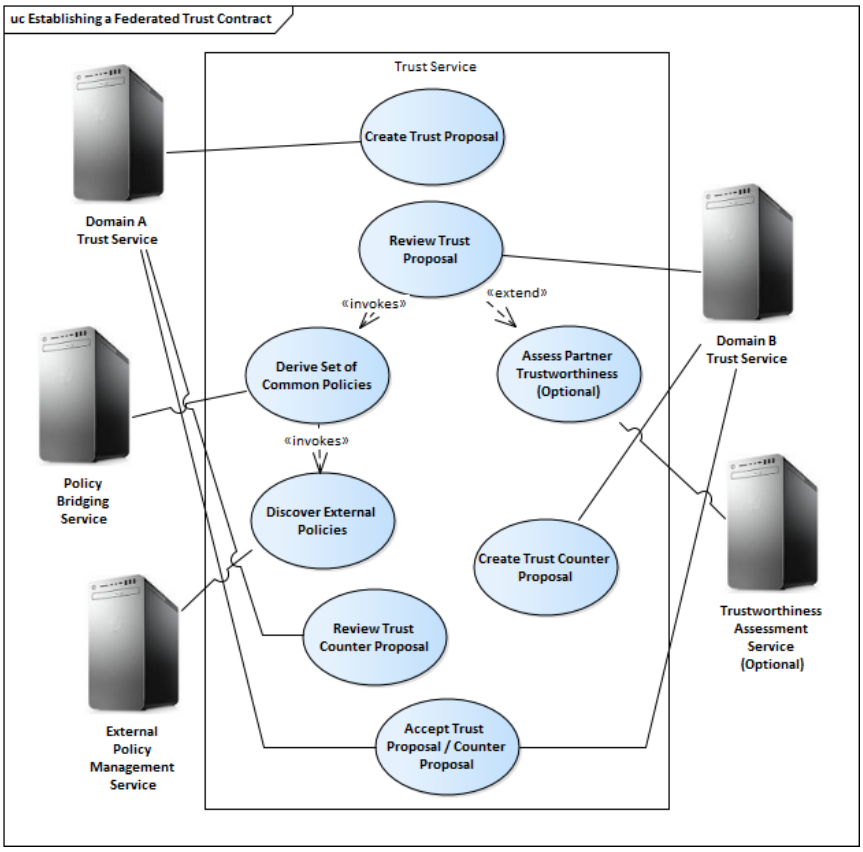

Figure 7: Trust Management Boundary View

2.4.1 Assumptions

2.4.2 Multiple architectural styles supported

This analysis requires that a number of different mechanisms for policy retrieval and reference be considered. The issue is especially relevant when looking at evaluating Privacy Policies with Client-specific attributes.

As an example, a base Privacy Policy may indicate that a Client can withdraw their consent to the disclosure of their Individually Identifiable Health Information (IIHI) from all but an identified list of providers or organizations. The Consent Directive is an instance of that policy, with real values for that list (or no values at all).

We have identified at least four different architectural mechanisms that may be needed for resolving the Client's consent directive, and at the conceptual level, will need to ensure that all four can be supported. These four mechanisms are:

- Each Consent Directive is executable and makes up part of the authoritative Access Control policy store. Consent Directives are evaluated as any other Security or Privacy policy would be.
- The base policy is constructed in such a way as to refer to an attribute obtained by the invocation of an external policy decision point which holds the Client's directives.
- The Access Control Service requests the executable Consent Directive from a trusted policy provisioning agent.

- The base Policy is constructed such that the required list of providers or organizations is retrieved as Access Control Decision Information (ADI) from a Privacy Policy or Consent Directive source.

This section identifies for different architectural mechanisms that may be needed to negotiate a federated authorization trust contract between two Domains.

When an initiating Domain (Domain A) intends to establish a Trust Framework for Federated Authorization with another Domain (Domain B), Domain A:

- Assembles a set of one or more Trust Policies from its Policy Administration Point [External Policy Management Service.]
- Creates a signed Trust Proposal.
- Sends to Trust Proposal Domain B.

Domain B receives and using a Policy Resolution Service, evaluates each Trust Policy in Domain A's Trust Proposal to determine whether each Trust Policy:

- Meets or exceeds a comparable Domain B Trust Policy.
  - If, after evaluation, Domain B determines that all of the Trust Policies included in Domain A's Trust Proposal meet or exceed Domain B's Trust Policies, then Domain B can accept Domain A's Trust Proposal by counter signing, thereby executing a Trust Contract to return to Domain A and submits the Trust Contract to the Trust Service.
- Does not match any of Domain B Trust Policies.
  - If, after evaluation, Domain B determines that none of the Trust Policies in Domain A's Trust Proposal match Domain B's Trust Policies, then Domain B can:
    - Reject Domain A's Trust Proposal by responding with Trust Proposal declined

2.4.3 Distributed Capabilities

There is an assumption that any of the identified capabilities or use cases may be distributed. The exercise of creating conformance profiles will determine the most appropriate "packaging" of behavior. Where applicable, each of the use cases is based on the assumptions of two domains: Domain "A" and Domain "B", with distinct access control policies, but which participate in a shared identity federation.

2.4.4 Actors

- Domain A Trust Service (Requestor)
- Domain B Trust Service (Data Owner)
- Policy Bridging Service
- External Policy Management Service
- Trustworthiness Assessment Service

2.4.5 Use Case TF-1: Draft Trust Proposal

Description

Draft a new or modified trust proposal.

Assumptions

- Domain A has a Trust Service that is able to communicate with the data owner's trust service.
- The domains have a communication mechanism over which a trust proposal can be submitted, and subsequent iterative communication can occur.

Actors

- Domain A Trust Service

Trigger Events

- Domain A has a set of users that require access to healthcare information owned by Domain B, or
- Use Case TF-7: Review Trust Counter Proposal returns a result indicating a need to modify the original request in order to be able to meet Domain B's data sharing requirements.

Pre-Conditions

- Domain A has an identified need for information owned by Domain B, and/or
- Domain A is responding to a trust counter-proposal submitted by the Domain B Trust Service.

Post-Conditions

- A new or modified, digitally signed, trust proposal is created and sent to the Domain B Trust Service.

2.4.6 Use Case TF-2: Review Trust Proposal

Description

The trust proposal is reviewed for completeness and compliance with Domain B's data sharing requirements. This review may trigger the involvement of additional services in order for additional compliance information.

Assumptions

The domains have a communication mechanism over which a trust proposal can be submitted, and subsequent iterative communication can occur

Actors

Domain B Trust Service

Policy Bridging Service (secondary)

Trustworthiness Assessment Service (secondary)

External Policy Management Service (indirect)

Trigger Events

Use Case TF-1: Draft Trust Proposal

Pre-Conditions

- A digitally signed trust proposal is received which includes policy information from Domain A Trust Service.
- The trust proposal includes identity information from Domain A.

Post-Conditions

- All policy and compliance information is received and used to determine if the trust proposal is either:
  - Acceptable as submitted (i.e. doesn't require a counter proposal).
  - Not acceptable as submitted and therefore:
    - Requires a counter proposal in order to exchange information, or
    - Policy and compliance information returned triggers a termination of the transaction.

2.4.7 Use Case TF-3: Derive Set of Common Policies

Description

Derive (negotiate) the set of common, domain-specific security and privacy policies required for trustworthy co-operation between collaborating domains

Assumptions

The set of policies necessary for establishing trustworthy co-operation between Domain A and B Trust Services are available or can be acquired.

Actors

Policy Bridging Service

External Policy Management Service (indirect)

Domain A Trust Service

Domain B Trust Service (indirect)**Trigger Events**

Use Case TF-2: Review Trust Proposal

Pre-Conditions

The result of Use Case TF-2, Review of Trust Proposal, is that the policies included in the trust proposal are sufficient to perform policy bridging.

Post-Conditions

Completed policy bridging information is returned to the Domain B Trust Service.

2.4.8 Use Case TF-4: Assess Partner Trustworthiness

Description

Determine trustworthiness of the requestor using event-driven security and behavior analytics.

Assumptions

There exists a Trustworthiness Assessment service that can perform event-driven security and behavior analytics.

Actors

Trustworthiness Assessment Service

Trigger Events

Use Case TF-2: Review Trust Proposal

Pre-Conditions

The result of Use Case TF-2, Review of Trust Proposal, is that the identity information included in the trust proposal is sufficient to perform the trustworthiness assessment.

Post-Conditions

Trustworthiness ADI is returned to the Domain B Trust Service and can be used to determine level of access allowable to Domain A via its trust service.

2.4.9 Use Case TF-5: Discover External Policy

Description

Discover external policies required for the trustworthy exchange of healthcare information between domains.

Assumptions

There is an External Policy Management service which contains policies and compliance information pertaining to Domain A.

Actors

External Policy Management Service

Trigger Events

Use Case TF-3: Derive Set of Common Policies

Pre-Conditions

The Policy Bridging Service determines a need for additional policy information not contained in the original trust proposal.

Post-Conditions

Policy and compliance information is returned to the Policy Bridging Service

2.4.10 Use Case TF-6: Draft Counter Proposal

Description

Create a digitally signed trust counter proposal.

Assumptions

- Domain B (the data owner) has a trust service that is able to communicate with Domain A's Trust Service (the requestor).
- The domains have a communication mechanism over which a trust proposal can be submitted, and subsequent iterative communication can occur
- The results of the analysis by the Trustworthiness Assessment and the Policy Bridging Service do not result in a complete termination of the transaction.

Actors

Domain B Trust Service

Trigger Events

Information returned from Use Case TF-2, Review Trust Proposal, indicates not acceptable as submitted and therefore indicates that a counter proposal should be sent to the Domain A Trust Service.

Pre-Conditions

- An initial trust proposal is received and reviewed.
- The Policy Bridging Service returns information specifying what changes need to be made to the original trust proposal in order to meet Domain B's requirements for sharing the requested information.

Post-Conditions

A digitally-signed counter-proposal is generated and returned to the Domain A Trust Service.

2.4.11 Use Case TF-7: Review Trust Counter Proposal

Description

The trust counter proposal is reviewed in order to determine Domain A's ability to meet Domain B's data sharing requirements.

Assumptions

The domains have a communication mechanism over which a trust proposal can be submitted, and subsequent iterative communication can occur

Actors

Domain A Trust Service

Trigger Events

Use Case TF-6: Draft Trust Counter Proposal

Pre-Conditions

A digitally signed trust counter proposal is received from the Domain B Trust Service.

Post-Conditions

- The trust counter proposal is:
  - Acceptable as submitted (i.e. doesn't require any modification).
  - The trust counter proposal is not acceptable as submitted and therefore:
    - Requires that Domain A Trust Service draft a modified trust proposal, or
    - Domain A Trust Service terminates the transaction.

2.4.12 Use Case TF-8: Accept Trust Proposal/Counter Proposal

Description

Both domain trust services digitally sign and accept the trust proposal or counter proposal as submitted thus establishing a Federated Trust Contract.

Assumptions

The domains have a communication mechanism over which a trust proposal can be submitted, and subsequent iterative communication can occur

Actors

Domain A Trust Service

Domain B Trust Service

Trigger Events

- A return of "Acceptable as Submitted" by either Use Case TF-2, Review Trust Proposal, or Use Case TF-7, Review Trust Counter Proposal.

Pre-Conditions

- Domain B Trust Service has an acceptable trust proposal that is already digitally signed by the Domain A Trust Service, or
- Domain A Trust Service has an acceptable trust counter proposal that is already digitally signed by the Domain B Trust Service.

Post-Conditions

A Federated Trust Contract is established as a result of having a trust proposal/counter proposal that is digitally signed by both the Domain A and Domain B Trust Services.

2.5 Healthcare Trust Framework Requirements

The table below summarizes all of the informational, functional, and quality requirements identified through review and analysis of the scenarios and use cases presented above.

Note: Where the requirements in Table 2 below identify healthcare-specific functionality or semantic content, those requirements are reflected in the Conformance section of this document.

Table 2: TF4FA Trust Service Baseline Requirements

ID	Requirement Title/Text	Healthcare Specific Component? Y/N	Functional / Semantic F/S	Implied Capability?	Functional Framework Requirement Map
TF1.0	TF4FA Trust Services	Description: Federated authorization is based on trust negotiated between domains and manifested in computable Trust Contracts that make the negotiated business and technical operational rules legally binding between federation domain members. The contracts are negotiated by trust framework services, each of which negotiates a specific aspect of the contract or provides a supporting service. The output of the Trust Services is the establishment of a Federated Authorization Domain, which 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.			
AC1-0	Cross Cutting Requirements	General requirements applicable to all components.			
ACG-3	Generate security audit records based on healthcare-specific security relevant events.	Y	S	- Recording security-relevant events in an audit trail - Support auditing of access control actions and administration. - The audit record produced by any service has to be conformant with the audit schema of the audit service	
ACG-4	Incorporate standard healthcare-specific access control information code sets per HL7 security and privacy domain models.	Y	S	This requirement will be solved by the use of semantic signifiers as input and output parameters in the capability tables. Semantic profiles may also bind the concrete	

ID	Requirement Title/Text	Healthcare Specific Component? Y/N	Functional / Semantic F/S	Implied Capability?	Functional Framework Requirement Map
				information models to the semantic signifiers.	
AC1-0	Domain A ACS	Description: The Domain A ACS acts on behalf of the initiator to submit a signed Trust Proposal/Contract as part of an extended access request.			
AC1-1	Provide access control decision information (ADI, i.e.: policy attribute values) to another service.	Y	F		ACFW 1.4.1
AC1-2	Request access control decision information (ADI, i.e.: policy attribute values) from another service.	Y	S	The ability to request or retrieve attributes / information / tokens / decision factors	ACFW 1.3.2.3
AC1-4	Ability to request or receive security credentials from a security credentialing service within or outside of ACS.	N	F/S	May be requesting one set of services and returning another. Ability to say "I don't have enough information" but need a different credential and the type.	ACFW 1.1.2 ACFW 1.1.3 ACFW 1.1.4 ACFW 1.2.7
AC1-7	Provide the capability to check if there are external policies with access control information (policy documents) that apply to the current request context.	N	F/S		ACFW 1.1.8 ACFW 1.1.9 ACFW 1.3.2.4

ID	Requirement Title/Text	Healthcare Specific Component? Y/N	Functional / Semantic F/S	Implied Capability?	Functional Framework Requirement Map
AC2-2	Support the capability to switch preplanned profiles of policy sets based upon purpose of use.	N	N	See AC2-8. This can occur in different ways, e.g. input from a user that is passed as a token, input from a user that causes an invocation of a submit event capability. Use case: Victim of Violence	ACFW 1.2.2 ACFW 1.4.2.1
AC2-5	Receive a request for an access control decision from another service	N	F/S	The way you would invoke the access control decision is to say "request an access control decision" The vocabulary for these rules will come from other groups like HL7 Community-Based Collaborative Care (CBCC) and the OASIS Cross-Enterprise Security & Privacy Authorization (XSPA) Technical Committee and be specified in the Semantic Profile section of this document. E.g.: - People - Structural or	ACFW 1.2.6 ACFW 1.3.2.1

ID	Requirement Title/Text	Healthcare Specific Component? Y/N	Functional / Semantic F/S	Implied Capability?	Functional Framework Requirement Map
				FunctionalRoles - Intended Use - Confidentiality - Location	
AC	Domain B ACS	Description: The Domain B ACS negotiates policy ADI with respect to Domain A Trust Proposals on behalf of Domain B protected information resources.			
AC2-6	Request or retrieve a policy decision from another policy decision service or access control service or other related service	N	F	Yes, No, I Don't Know (3-states)	ACFW 1.1.2 ACFW 1.1.8 ACFW 1.1.9 ACFW 1.1.10 ACFW 1.3.1.2 ACFW 1.3.2.4
AC2-7	Request a machine-readable policy document from another service.	Y	F/S	- Request access control info, decision factors - Request access control policies - List access control policies	ACFW 1.1.2 ACFW 1.1.8 ACFW 1.1.9 ACFW 1.1.10 ACFW 1.3.1.2 ACFW 1.3.2.4
AC2-8	Receive a request for a machine-readable policy document from another service.	Y	F		ACFW 1.4.2.2
AC2-9	Support exchange of security and privacy policy documents with other access control service.	Y	F	Ensure that the same policy that is distributed over more than one ACS provides the same access control results everywhere at the same point in	ACFW 1.1.2 ACFW 1.1.3 ACFW 1.1.4 ACFW 1.1.6 ACFW 1.1.8 ACFW 1.1.9 ACFW 1.1.10 ACFW 1.1.11

ID	Requirement Title/Text	Healthcare Specific Component? Y/N	Functional / Semantic F/S	Implied Capability?	Functional Framework Requirement Map
				time. This implies a number of functions: a) notification of policy updates b) distribution of updated policies (push or pull) c) synchronized policy activation / deactivation	ACFW 1.3.2.4 ACFW 1.4.2.4
AC2-11	Respond to a request for a machine-readable policy document from another service.	Y	S	Mike to provide text	ACFW 1.4.2.2 ACFW 1.4.2.3 ACFW 1.4.2.4
TF1.4	Policy Bridging Service	Description: The Policy Bridging Service harmonizes the local polices of the partner authorities into a unified Federation Policy for use within the Federated Authorization Domain being established. The service does this by exchanging the partners' class policy attributes and deriving (negotiating) the highest possible level of mutual agreement between them.			
TF 1.1.1	Harmonize Authorization Policy Provide the capability to harmonize Domain Partners' Authorization policies.	N	F	Harmonize (negotiate) the local Authorization polices of the partner authorities into a unified Federated Policy, which both partners agree to use without exception for all applicable access requests within the Federated Domain.	ACFW-1.1.4 ACFW-1.1.5 ACFW-1.1.8 ACFW-1.1.9

ID	Requirement Title/Text	Healthcare Specific Component? Y/N	Functional / Semantic F/S	Implied Capability?	Functional Framework Requirement Map
TF 1.1.2	Harmonize Refrain Policy Provide the capability to harmonize Domain Partners' Refrain policies	N	F	Harmonize (negotiate) the local Refrain polices of the partner authorities into a unified Federated Policy, which both partners agree to use without exception for all applicable access requests within the Federated Domain.	ACFW-1.1.4 ACFW-1.1.5 ACFW-1.1.8 ACFW-1.1.9
TF 1.1.3	Harmonize Obligation Policy Provide the capability to harmonize Domain Partners' Obligation policies.	N	F	Harmonize (negotiate) the local Obligation polices of the partner authorities into a unified Federated Policy, which both partners agree to use without exception for all applicable access requests within the Federated Domain.	ACFW-1.1.4 ACFW-1.1.5 ACFW-1.1.8 ACFW-1.1.9
TF 1.1.4	Harmonize Delegation Policy Provide the capability to harmonize Domain Partners' Delegation policies.	N	F	Harmonize (negotiate) the local Delegation polices of the partner authorities into a unified Federated Policy, which both partners	ACFW-1.1.4 ACFW-1.1.5 ACFW-1.1.8 ACFW-1.1.9

ID	Requirement Title/Text	Healthcare Specific Component? Y/N	Functional / Semantic F/S	Implied Capability?	Functional Framework Requirement Map
				agree to use without exception for all applicable access requests within the Federated Domain.	
TF 1.2	External Policy Management Service	Description: The External Policy Management Service is a publicly-facing service that allows domains to post their local access control policies and other relevant or requested trust information as necessary. Once posted, partners attempting to establish trust between them may access each other's trust information from the service.			
TF 1.2.1	Discover External Policy Management Service Provide the capability to discover (find) the External Policy Management Service	N	F	Discovery needs to be facilitated by the External Policy Management Service. Discovery by a potential user of the Service may in advance of needing posted information or in real time as information is needed. Examples of discovery mechanisms include but are not limited to the External Policy Management Service distributing a Uniform Resource Locator (URL) to a known set of	ACFW-1.1.11

ID	Requirement Title/Text	Healthcare Specific Component? Y/N	Functional / Semantic F/S	Implied Capability?	Functional Framework Requirement Map
				partners for configuration into their systems, and by ongoing broadcasting of its existence and location so any system can discover it without a priori knowledge of the Service.	
TF 1.2.2	Post Trust Information Provide the capability to Post trust information to the External Policy Management Service	N	F	Once discovered, a partner may post any initial set of trust information to the External Policy Management Service. Posted trust information must be in a standard format known to all and must use a standard vocabulary agreed to by all. Posting of trust information may be driven by the information owner or by a request to post from a current or potential trust partner.	ACFW-1.1.8 ACFW-1.1.10
TF 1.2.3	Update Posted Trust Information Provide the capability to update trust information already posted to the	N	F	Some or all of already-posted trust information may be updated as necessary. Additional trust	ACFW-1.1.8 ACFW-1.1.10

ID	Requirement Title/Text	Healthcare Specific Component? Y/N	Functional / Semantic F/S	Implied Capability?	Functional Framework Requirement Map
	External Policy Management Service			information (not already posted) may also be added. Updating of trust information may be driven by the information owner or by a request to post from a current or potential trust partner.	
TF 1.3	Trustworthiness Assessment Service	Description: The Trustworthiness Assessment Service is an event-driven service to perform continuous assessment and analysis of Initiator behavior. Adaptive behavior analytics is used to assess whether current trust should be continued or modified.			
TF 1.3.1	Update Initiator Trust Analytics Provide the capability to analyze initiator behavior based on continuous ongoing assessment.	N	F	Provides the ability to determine if current trust assessment has changed by analysis of behavioral history (e.g. lawsuits, breaches, adverse reporting, loss of certifications)	ACFW-1.1.4 ACFW-1.1.10
TF 1.3.2	Post Behavioral Trust Information Provide the capability to post behavioral updates to the Domain B Access Control Service.	N	F	The ACS uses posted information as Trust Decision Information to verify or remove eligibility for information exchange.	ACFW-1.1.4 ACFW-1.1.10
TF 1.4	Domain Trust Service (DTS)	Description: The Domain Trust Service is responsible for creating and signing			

ID	Requirement Title/Text	Healthcare Specific Component? Y/N	Functional / Semantic F/S	Implied Capability?	Functional Framework Requirement Map
		Trust Proposals and Counter-Proposals leading to a Trust Contract.			
TF 1.4.1	Submit Trust Proposal.	Y	F/S	The DTS creates/accepts and signs a Trust Proposal	ACFW-1.1.4 ACWF-1.1.5 ACWF-1.1.8 ACFW-1.1.10
TF 1.4.2	Submit Counter Proposal	Y	F/S	The DTS creates/accepts and signs a Counter-proposal	ACFW-1.1.4 ACWF-1.1.5 ACWF-1.1.8 ACFW-1.1.10

3 FUNCTIONAL FRAMEWORK VIEWPOINT

3.1 Executive Summary

The primary goal of a trust framework is to establish the legal, ethical, social, organizational, psychological, functional, and technical factors under which exchange of protected information may occur. This involves identifying aspects of exchange, binding on all parties that occur prior to the actual determination of whether or not information access is to be allowed (access control). The service is intended to leverage trust information from existing frameworks leveraging trustworthy assertions from sources of authority.

Unauthorized operations involving a computer or communications system are frequently subdivided into classes known as: unauthorized use; disclosure; modification; destruction; and denial of service [ISO 10181-3]. In addition, accesses may either be to a system (i.e. to an entity that is the communicating to a system or part of a system) or within a system. The information items that need to be presented to obtain the access, as well as the sequence of operations to request the access and for notification of the results of the access, are considered to be within the scope of this functional model. [ISO 10181-3].

3.1.1 Service Overview

The trust framework service model provides a logical view that encapsulates like requirements into capabilities. The functional framework model is not implementation design; in fact, functional models are implementation and technology agnostic. Relative to the Business Viewpoint, the functional framework model viewpoint provides more detail.

The use of a Trust Framework can facilitate greater security access control cooperation, information sharing, consistency, and scalability. Trust Framework capabilities are instantiated in a domain policy, which is a written agreement where all involved parties commit themselves to a specified set of policies. The basic part of the domain policy contains descriptions of the actual legal framework, including rules and regulations. Trust Frameworks include organizational and administrative framework, functionalities, claims and objectives, the principals involved, agreements, rights, duties, and penalties. Also included are the technological solutions

implemented for the creation, collection, storage, processing, disclosure, retention, transmission, and use of data in applications within the security and privacy policy domains.

3.1.2 Trust Framework Model

The HL7 PASS ACS Functional Framework Service is illustrated in Figure 8 below. Use of a trust framework can facilitate greater security access control cooperation, information sharing, consistency, and scalability.

The TF4FA model elaborates on the HL7 PASS ACS Trust Framework Service by providing a standards-based conceptual approach to the HL7 PASS ACS Trust Framework Service capabilities so that trust can be established between domains before general access control processing and enforcement is performed.

3.2 Preconditions for Participation

3.3 Please refer to 1.2.2 for pre-conditions for participation. Capabilities of the PASS ACS Trust Service

Pass ACS Trust Framework and capabilities form the foundation for this document and are adopted and expanded upon throughout, adding further detail.

3.3.1 Structure of the Service

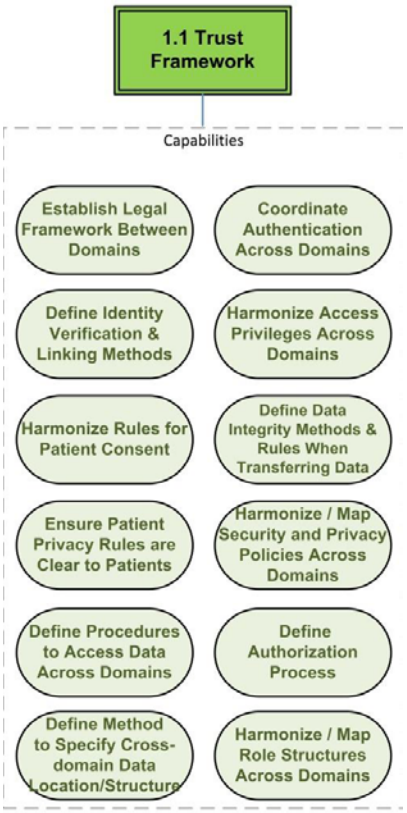

Figure 8: HL7 PASS ACS Trust Framework Service

Figure 9 describes the structure of the Trust Framework service in terms of included capabilities. See [PASS ACS] for definition and description of the service in the context of general access control.

3.3.2 Implementation Considerations

An implementation of the Access Control Service may need to use other Security and Privacy Architecture services to ensure the authenticity of information exchanged during the access control process (e.g. exchange of access control information or access policy rules) and to securely store access *control information and policies. Examples of other services that might be invoked are Encryption Service, Electronic Signature Service, and Authentication Service. Additional supporting services likely to be invoked include Audit Service, Time Synchronization, Security Labeling Service, and Privacy Protective Service.*

The Access Control Service is aligned with industry standards, directly supports business needs and involves *several phases. Upon receipt of an access request (encapsulated in a Policy Proposal) submitted by an Initiator, the Domain Trust Service begins processing. The access request is aimed at a particular Target (resource) and includes Initiator Access Control Information (ACI). Examples of Initiator ACI include (a) access control identity of an individual; (b) identifier of the hierarchical group in which membership is asserted; (c) identifier of the functional group in which membership is* asserted; (d) identifiers of roles that may be taken; (e) sensitivity markings; and (f) integrity markings. The various Initiator ACI support several different Access Control Schemes that can be implemented (e.g. based on access control lists, capabilities, labels, and context).

The Policy Enforcement Point (PEP) within the AEF invokes the Policy Decision Point (PDP) within the Access Decision Function (ADF) to make an access decision, which the PEP will then enforce. The PDP gathers all necessary Access Control Decision Information (ADI) derived from ACI associated with all applicable elements (e.g. Initiator, Target, Access Request), access policies, security and privacy policies, consent directives, contextual information, and if necessary, any stored ADI from previous access control decisions. The PDP processes all the gathered information in order to make a decision. When conflicts arise between inputs, the PDP uses previously-configured rules (e.g. precedence rules) to resolve the conflicts. Finally, the PDP makes an access decision based on all reconciled information. The PDP then obtains any applicable obligations (e.g. create an audit record of this access) associated with the Subject and access request. The PDP then returns the decision, advice, and obligations to the PEP for enforcement. If circumstances warrant, the PEP may allow access regardless of normal policy stipulations in order to support emergency (break-the-glass) situations. The PDP may save ADI generated from the current access request for use in future access requests.

3.4 Business Scenario

See Section 2.3 Scenarios, in the Business Viewpoint section.

3.4.1 Capability Requirements

Table 3: Capability Requirements

ID #	Service/Sub-service Title	Service/ Sub-service Description		Source	Bus Reqs
	Requirement Title	Requirement Text	Guidance[8]		
ACFW-1.1	Trust Framework	Description: Trust Framework capabilities are instantiated in a domain policy, which is a written agreement where all domain policy contains descriptions of the actual legal framework, including rules and regulations. Trust Frameworks include organizational and administrative framework, functionalities, claims and objectives, the principals involved, agreements, rights, duties, and penalties. Also included are the technological solutions implemented for the creation, collection, storage, processing, disclosure, retention, transmission, and use of data in applications within the security and privacy policy domains.		ISO 22600-1	
ACFW-1.1.1	Establish Legal Framework Between Domains	Provide the capability to establish a legal framework across participating domains.	The objective is to describe the actual legal framework including rules and regulations, responsibilities, and liabilities. The legal framework is agreed upon by all participating domains and specified in a domain policy.	ISO 22600-1	
ACFW-1.1.2	Coordinate Authentications Across Domains	Provide the capability to coordinate and standardize authentication across participating domains.	Authentication of users/roles should be based on PKI according to ISO 17090. When different methods are used by participating domains, an approach should be agreed upon by all participating domains and specified in a domain policy. For cases where the participating domains cannot agree upon a common standardized authentication system, ISO 22600 specifies a number of stipulations to be met.	ISO 22600-1	AC1-4 AC2-6 AC2-7 AC2-9
ACFW-1.1.3	Define Identity Verification &	Provide the capability to link	The domain policy defines the identity validation and/or	ISO 22600-1	AC1-4 AC2-9

[8] Guidance narrative is taken nearly verbatim from the authoritative source(s) specified in the Source column.

ID #	Service/Sub-service Title	Service/ Sub-service Description		Source	Bus Reqs
	Requirement Title	Requirement Text	Guidance[8]		
	Linking Methods	and verify identities across participating domains.	verification methods used in the domains, including identity proofing for methods used in the security and privacy policy domains for the identification of principals such as persons (patients, healthcare professionals, health professionals, etc.), organizations, systems, devices, applications, components, etc. If different identification systems are used, the applied system has to be defined. Linking, mapping, or conversion mechanisms need to also be defined. In that context, the use of a unique patient ID as well as namespace-related master patient indexes and the use of a patient identification service should be considered and specified.		
ACFW-1.1.4	Harmonize Access Privileges Across Domains	Provide the capability to harmonize access privileges across participating domains.	Rules for access privileges are agreed upon by participating domains and specified in the domain policy. The circumstances allowing access to the information in another domain are described in ISO 22600-2.	ISO 22600-1	AC1-4 AC2-9 TF1.1.1 TF1.1.2 TF1.1.3 TF1.1.4 TF1.3.1 TF1.3.2 TF1.4.1 TF1.4.2
ACFW-1.1.5	Harmonize Rules for Patient Consent	Provide the capability to harmonize patient consent rules across participating domains.	The rules for patient consent have to be harmonized. If harmonization is not possible, principles have to be defined ruling how differences shall be bridged. The rules for patient consent are agreed upon by all	ISO 22600-1	TF1.1.1 TF1.1.2 TF1.1.3 TF1.1.4 TF1.4.1 TF1.4.2

ID #	Service/Sub-service Title	Service/ Sub-service Description		Source	Bus Reqs
	Requirement Title	Requirement Text	Guidance[8]		
			participating domains and specified in a domain policy.		
ACFW-1.1.6	Define Data Integrity Methods & Rules When Transferring Data	Provide the capability to define data integrity methods for data being transferred across participating domains.	The methods and rules for checking the integrity of data shall be defined in order to detect unauthorized modification of data during transfer between the participating domains. The rules and techniques for such integrity check are agreed upon by all participating domains and specified in a domain policy.	ISO 22600-1	AC2-9
ACFW-1.1.7	Ensure Patient Privacy Rules are Clear to Patients	Provide the capability to ensure patient privacy rules are clear to patients.	Patient privacy is a key issue in communication across policy domain boundaries, and especially in trans-border information exchange. In order to gain a patient's full confidence with the information transactions, it is of utmost importance that the rules are clear and easily understood by the patients. The rules and techniques for ensuring clarity of patient privacy rules are agreed upon by all participating domains and specified in a domain policy.	ISO 22600-1 HL7 Patient Friendly Language	
ACFW-1.1.8	Harmonize / Map Security and Privacy Policies Across Domains	Provide the capability to harmonize privacy policies across participating domains.	Security and privacy policy domains are distinguished by their policies. Ideally, the communicating and cooperating security and privacy domains can commit to one and the same security model represented by a harmonized policy. This is the primary goal, and the security standards defined at both ISO [9]are the primary tools for achieving this.	ISO 22600-1	AC1-7 AC2-6 AC2-7 AC2-9 TF1.1.1 TF1.1.2 TF1.1.3 TF1.1.4 TF1.2.2

[9] See Volume 1, Appendix C under 'reference standards'

ID #	Service/Sub-service Title	Service/ Sub-service Description		Source	Bus Reqs
	Requirement Title	Requirement Text	Guidance[8]		
			If such harmonization is not possible, the domain policy specifies which policy can be considered equivalent for which role, information, action, and purpose. For each role, information, action, and purpose, a set of policies has to be defined. In cases where policies cannot be processed by the systems involved, security levels have to be defined including the related rules and the equivalences between them. See also ISO 22600-2		TF1.2.3 TF1.4.1 TF1.4.
ACFW-1.1.9	Define Procedures to Access Data Across Domains	Provide the capability to define procedures to access data across participating domains.	The domain policy defines the procedure of accessing data across participating domain boundaries. For different access modes such as read-only, transfer, process, or communicate, accessible information might be different. Therefore, information needs to be identifiable at the granularity level needed.	ISO 22600-1	ACG-2 AC1-7 AC2-6 AC2-7 AC2-9 TF1.1.1 TF1.1.2 TF1.1.3 TF1.1.4
ACFW-1.1.10	Define Authorization Process	Provide the capability to define the authorization process internally and across participating domains.	The authorization process is defined in the domain policy both internally to the security and privacy policy domain and between the interconnected domains.	ISO 22600-1	AC2-6 AC2-7 AC2-9 TF1.2.2 TF1.2.3 TF1.3.1 TF1.3.2 TF1.4.1 TF1.4.2
ACFW-1.1.11	Define Method to Specify Cross-domain Data Location/Structure	Provide the capability to define the method to	In order to secure the information retrieval, location and data structure of applications have to be	ISO 22600-1	AC2-9 TF1.1.4

ID #	Service/Sub-service Title	Service/ Sub-service Description		Source	Bus Reqs
	Requirement Title	Requirement Text	Guidance[8]		
		specify the location and structure of data across participating domains.	specified and understood by all parties. The domain policy contains detailed information about the location and structure of data, uniquely described by identifiers such as URLs and/or object identifiers (OIDs).		
ACFW-1.1.12	Harmonize / Map Role Structures Across Domains	Provide the capability to map and harmonize role structures across participating domains.	Roles are defined within each security and privacy policy domain. Privileges as well as contextual and environmental conditions are defined in policies that are bound to one or more roles. Role assignments and assertions are essential parts of the solution for the final policy bridging.	ISO 22600-1	

4 INFORMATIONAL VIEWPOINT

4.1 Business Rules / Constraints

None identified

4.2 Information Model

Information Models provide the basis for semantic content for trust. This section is concerned with the types of information as well as the constraints on and uses of the information.

4.2.1 Trust Framework Information Model

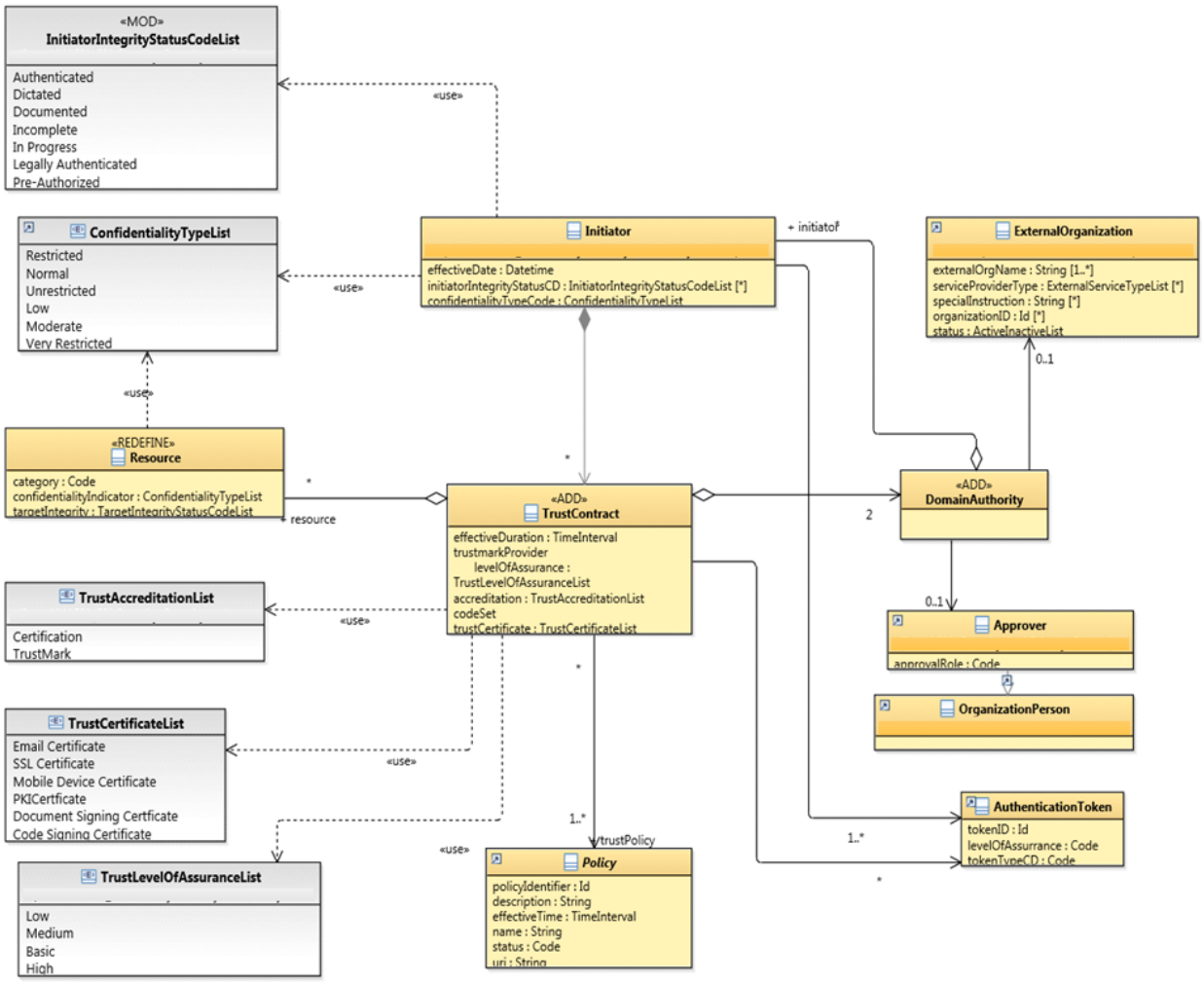

Figure 9: Federated Domain Trust Framework Model

Figure 10 summarizes the relationships among a Trust Contract and its environment. Trust Contracts make the business and technical operational rules of a domain legally binding upon its members, subject to jurisdictional, organizational, and privacy policies that apply equally to all members. Trust Contracts can have a time limit, after which a new, complete Trust Contract must be established.

4.2.2 Trust Policy Information Model

As noted in Section 1.1 the policy agreed upon by participating domains is derived from three policy categories: organizational policy, jurisdictional policy, and subject of care policy. In supporting all three policy categories, the TF4FA Policy Class Model defines an information model that ensures an implemented Federated Domain is user-centric (e.g. patient preferences are accounted for and processed accordingly so that owners of protected information maintain control over the sharing and use of their information).

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 it can provide sharable, stable, and organized structure of information requirements for the domain context. 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.

This document adopts the [ISO 22600-2] information model. However, the TF4FA Policy Class Model includes only ISO 22600-2 policy relevant to deriving authorization-related trust between participants as a precursor to access control processing, which is out of scope for this document. Accordingly, ISO 22600-2 Basic Policy is in scope for this document. Out of scope for this document are ISO 22600-2 Meta Policy (constraints over a set of policies) and Composite Policy (groupings of related policy specifications within syntactic scopes), both of which are used during access control processing.

This information model is complete enough to enable the development of downstream platform-independent models such as 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).

4.3 Trust Policy Information Model

The policy information model is a core construct that serves to establish access control related Federated Policy via TF4FA policy services. The policy information model captures and integrates all the policy elements necessary for federated authorization.

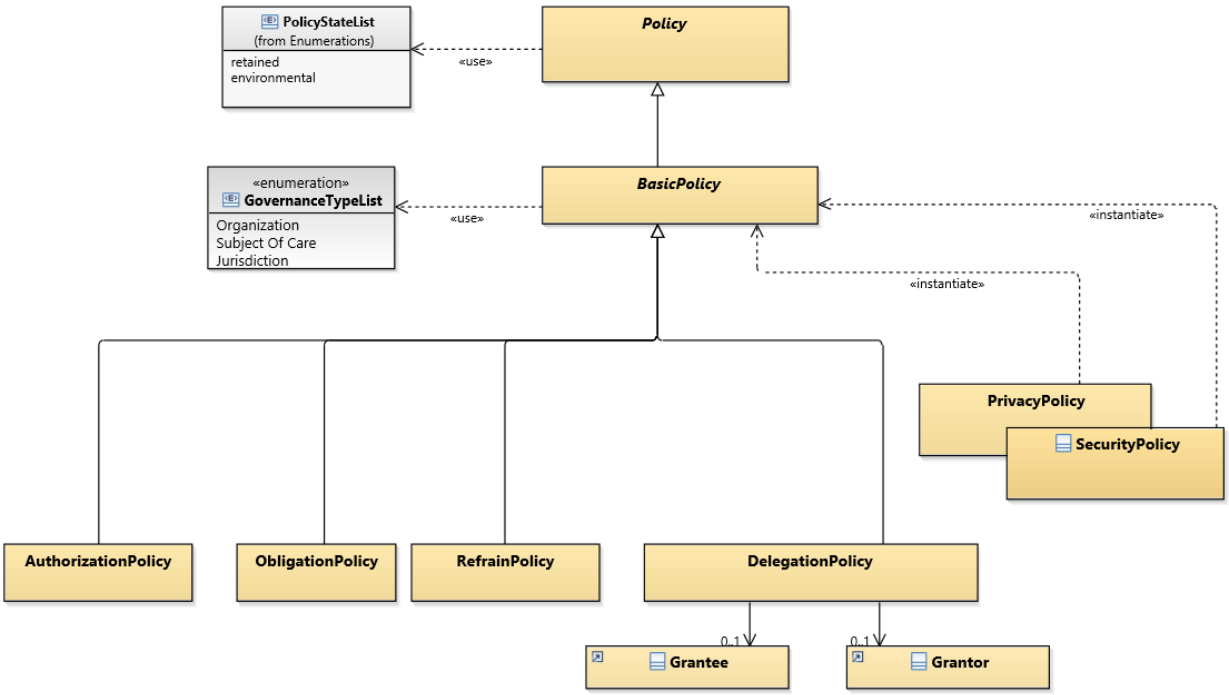

Figure 10: Federated Trust Policy Information Model (Derived from ISO 22600)

Figure 11 Trust Policy Information Model is a construct that shows access control related federated policy via policy services. The policy information model captures and integrates all the policy elements necessary for federated authorization. Security and privacy policies are instantiated from the core Basic policies, with the overlap of security policy and privacy policies representing the close relationship between them. Privacy policy contains a set of rules that are intended to be enforced by security systems.

The model focuses on Basic policy adopted from [ISO 22600-2]. Clarifications have been added and are adopted from other standards such as [ISO 10181-3] and other information models such as the HL7 Domain Analysis Model (DAM), which are incorporated herein by reference. The clarifications include use of *PolicyStateList*, use of *GovernanceTypeList*, and highlighting that security and privacy policies are instantiations of the core Basic polices. In addition, the [ISO 22600-2] abstract Policy class has been retitled to Federated Policy to reflect the federated nature of TF4FA.

As Figure 11 shows, security policy and privacy are derived (instantiated) from the core Basic policies. The overlap of security policy and privacy policy represents the close relationship between them. There is some overlap between security policy and privacy policy, and in some cases, they may address the same activities.

Privacy policy 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.[10] Privacy policy represents:

- A territorial authority that may be issuing privacy policies for a territory. [HL7 DAM]

[10] A Consent Directive is a record of a Subject of Care's 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]

- An organization that may be issuing privacy policies. [HL7 DAM]
- A set of privacy consent directives issued by a consenter on behalf of self or someone else. [HL7 DAM]

The sub-sections that follow explain and expand upon the main level classes. In addition, each subsection specifies where it was derived from.

4.3.1 Class: Federated Policy

This is the abstract class from which all concrete policy classes in this policy information model are derived and instantiated. Because this class is abstract, it cannot be instantiated as a security policy for healthcare. However, it specifies the properties reused by all policies. [HL7 DAM]

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]

Federated Policy uses a *PolicyStateList* to enumerate policy states including but not limited to retained policy (i.e. policy held over from a previous access control decision for subsequent use) and environmental policy (e.g. time of day, initiator location). These policy states derive from [ISO 10181-3].

This class is derived from [ISO 22600-2] and [HL7 DAM].

4.3.2 Class: 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 "plan or course of action adopted for providing computer security." [HL DAM]

Basic 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. Privacy policy is controlled by the Subject of Care.

Basic Policy includes four core types of policies (Authorization Policy, Refrain Policy, Obligation Policy, Delegation Policy) from which security policy and privacy policy are instantiated.

Basic policies cannot contain other policies. Although they usually need an explicit subject an exception is when a Basic Policy is specified as part of a role, in which case the subject domain of the role/clearance is the implicit subject.

This class is derived from [ISO 22600-2] and [HL7 DAM].

4.3.3 Class: 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]

For both positive and negative authorization policies, the specification of the following policy elements is required. An authorization policy must contain the following policy elements (adapted from [PONDER]):

- subject (except in roles)
- target
- action (roles only)

- rule (clearances only)[11]

Authorization Policy is a specialization of a Basic Policy.

This class is derived from [ISO 22600-2] and [HL7 DAM].

4.3.4 Class: 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. [HL7DAM]

A Refrain Policy must contain the following policy elements (adapted from [PONDER]):

- subject (except in roles)
- action (roles only)
- event
- rule (clearances only)

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

Authorization Policy is a specialization of a Basic Policy.

This class is derived from [ISO 22600-2] and [HL7 DAM].

4.3.5 Class: Obligation Policy

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]

An obligation policy must contain the following policy elements (adapted from [PONDER]):

- subject (except in roles)
- action (roles only)
- event
- rule (clearances only)

Obligation Policy is a specialization of the "Basic Policy" class.

[11] Rules are added to account for attribute-based access control which include the subject, target and a rule that links them

This class is derived from [ISO 22600-2] and [HL7 DAM].

4.3.6 Class: 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.

One or more positive authorization and/or delegation policies must always be associated with a delegation policy (both positive and negative). The only required policy element for a delegation policy is the specification of a grantee. Subjects and targets, if not specified, default to the aggregated subjects and targets of the associated authorization/delegation policies. If actions to be granted are not specified, they default to those of the associated authorization/delegation policies. [PONDER]

Delegation Policy is a specialization of the "Basic Policy" class.

This class is derived from [ISO 22600-2] and [HL7 DAM].

4.3.7 Class: Grantee

Grantees are the objects to whom access rights can be delegated. [PONDER]

A Grantee is not necessarily an authority. A Grantee may be a client, substitute decision maker, or an organization. For example, in the case of substance abuse related information, under certain conditions the authority to provide, withhold, or withdraw consent to the disclosure of the information is granted to a client. [HL7 DAM]

This class is derived from [ISO 22600-2] and [HL7 DAM].

4.3.8 Class: Grantor

Grantors are the subjects who can delegate access rights. [PONDER]

This class is derived from [ISO 22600-2] and [HL7 DAM].

4.3.9 Class: Access Control Information Policy

Access control information (ACI) is any information used for access control purposes, including contextual information [ISO 10181-3]. This class is derived from [ISO 10181-3]. Within the Trust Framework, ACI refers to policies about such information. For example, a Trust Contract may specify that the parties have agreed to use HL7 standard Attribute Based Access Control clearances to express user assertions of privilege to access HL7 classified data

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]

In actual operation, ACI must be bound to an element. Accordingly, the types of ACI include initiator, resource, access request, operation, operand and contextual information. The essential scenario is an Initiator seeking access to a protected Resource, where ACI are inputs into the access control decision. Which ACI is required depends upon the chosen security policy. [ISO 10181-3]

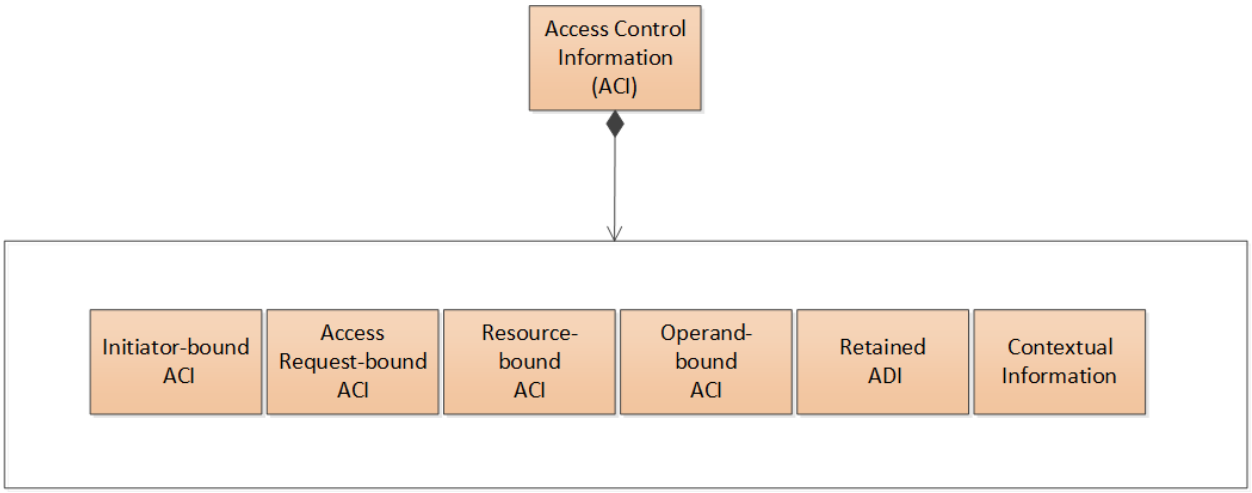

Figure 11: Expanded View of ACI Class

4.3.10 Class: Initiator-bound ACI

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

This class is derived from ISO 10181-3.

4.3.11 Class: 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]

This class is derived from ISO 10181-3.

4.3.12 Class: Resource-bound ACI

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

This class is derived from ISO 10181-3.

4.3.13 Class: 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.

This class is derived from ISO 10181-3.

4.3.14 Class: 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]

This class is derived from ISO 10181-3.

4.3.15 Class: 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 to non-privilege providers in extraordinary circumstances such as a disaster. [ISO 10181-3]

This class is derived from ISO 10181-3.

4.4 Semantic Signifiers

A semantic signifier is used to specify constraints on the information constructs that serve as payloads within service operations. It is the identification of a named set of information descriptions that are supported by one or more operations. The reference points for associated conformance statements occur at the computational model interface where the semantic signifier is specified as an input or output required by the contract.

4.4.1 Trust Proposal Message

Purpose

The Access Request Message encapsulates the information needed to request and enforce an access control decision. The Access Request Message consists of three first-order business concepts: User, Resource, and Operation. User and Operation are identified in both Privacy and Security DAM's, while Target characteristics may be specified in policies, but a particular resource identifier will not be.

Attributes and assertions associated with a particular request message may be mapped to policy attributes as indicated (e.g. Purpose of Use, an attribute of Basic Policy is represented as a request attribute that is used as Access Decision Information.

The healthcare-specific semantic elements are identified in Figure 12, below.

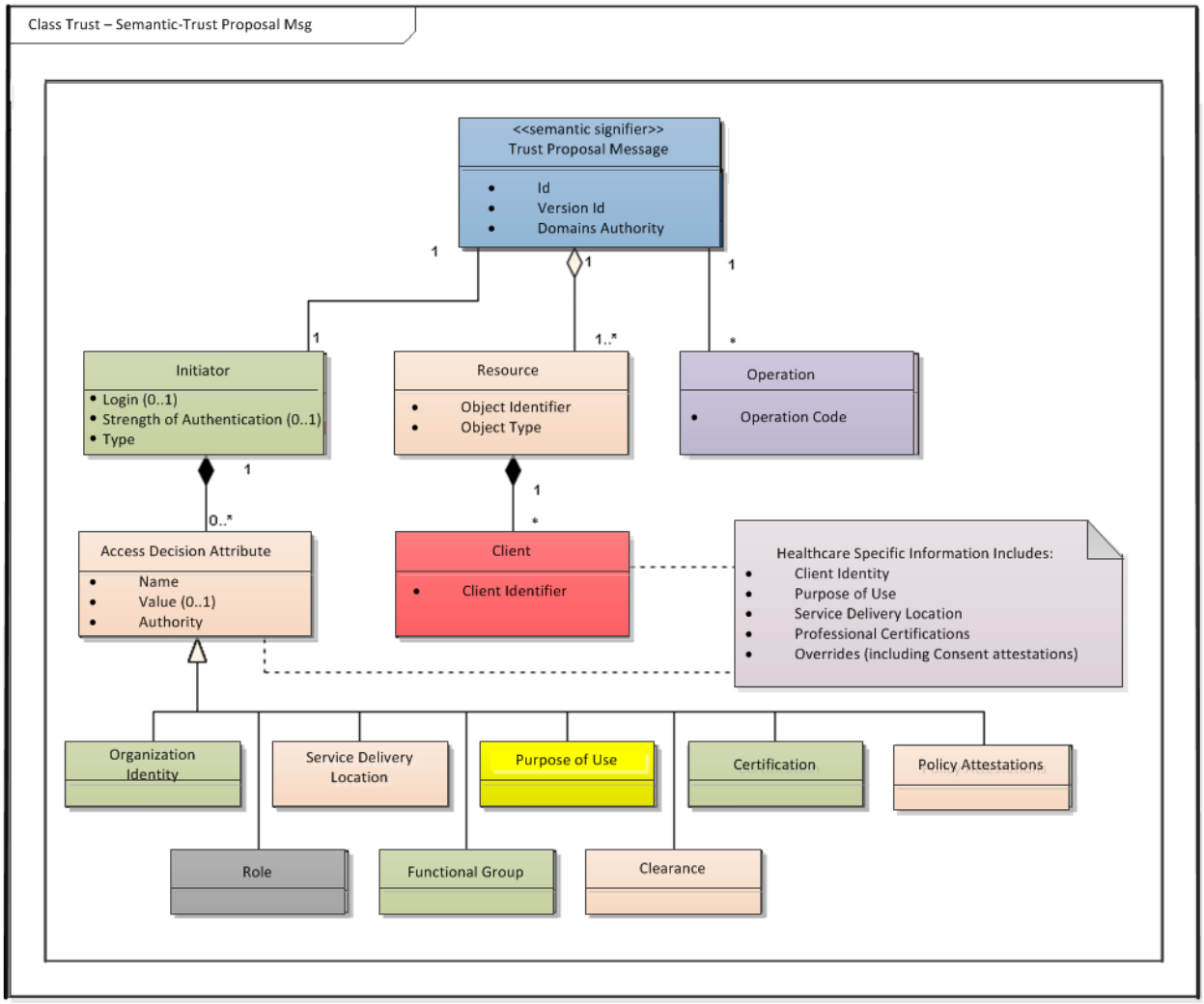

Figure 12: Trust Proposal Message

Details of the Access Request Message business concepts and attributes are as follows:

Table 4: Access Request Message Business Concepts and Attributes

Concept	Attribute	Description
Initiator	Identity	A unique identifier associated with the Initiator or Service Requestor. Some identity federation mechanism is assumed to enable mapping of requestor identities to User identities specified in any policy. An Initiator may be a human or a machine actor. Mandatory.
Initiator	Authentication Strength	A coded concept indicating the strength of the authentication process used to identity the User. This attribute is associated directly with a Security Policy; however, it is always in relation to the Initiator making a specific request. Optional.

Concept	Attribute	Description
Assertion / Attribute	Name	The name (or type) associated with the assertion or attribute.
Assertion / Attribute	Value	The optional value of the attribute. Assertions generally will not be associated with values.
Assertion / Attribute	Authority	The identity of the authority making the assertion or verifying the attribute.
Resource	Object Identifier	A unique identifier associated with the resource that is being accessed.
Resource	Object Type	The type of resource being requested. Object types are coded concepts from the HL7 V3 RBAC Constraint Catalogue. Optional.
Client	Client Identifier	A unique Client identifier, usually used to identify privacy policies or consent directives specific to that identifier. In order to support distributed policy stores, some federation mechanism will have to be implemented in order to assure identity correlation. Clients are associated only with the Resource being requested. Optional.
Operation	Operation Code	This is the coded concept from the HL7 V3 RBAC Constraint Catalogue. Mandatory.

Assertions and attributes provide for flexibility and extensibility in the implementation of components that produce and consume the Access Request Message, however semantic interoperability requires that we specify the particular attributes that may be necessary for interoperability in the healthcare environment.

Table 5: Optional Attributes

Attribute	Description
Organization Identity	The unique identity associated with the organization that is responsible for the actions of the Requestor.
Service Delivery Location	The location from which the Requestor is providing service.
Purpose of Use	The specific purpose for the request. This might be assumed to be treatment/provision of care, may be determined by the Requestor's functional or structural role in an RBAC access control environment, or specifically identified here. Coded concept.
Role	The structural role that the User is operating in for this request.
Functional Group	The functional role that the User is operating in for this request.

Attribute	Description
Certification	Any professional certification credentials that may be required for the request. Usually provided by a jurisdictional or professional body.
Policy Attestation	(Optional). Machine-driven assessment of an information exchange partner's conformance/non-conformance to legal, ethical, social, organizational, psychological, functional, and technical factors assumed or known from behavioral analytics and continuous event driven performance factors deemed relevant to retaining trust.

4.4.2 Policy Selection Criteria

Purpose

Policy Selection Criteria consists of the semantics used to select one or more policies, specifically for the purpose of subsequent evaluation. In this context, there is a finite set of criteria that would be reasonable to use in order to facilitate the policy selection process.

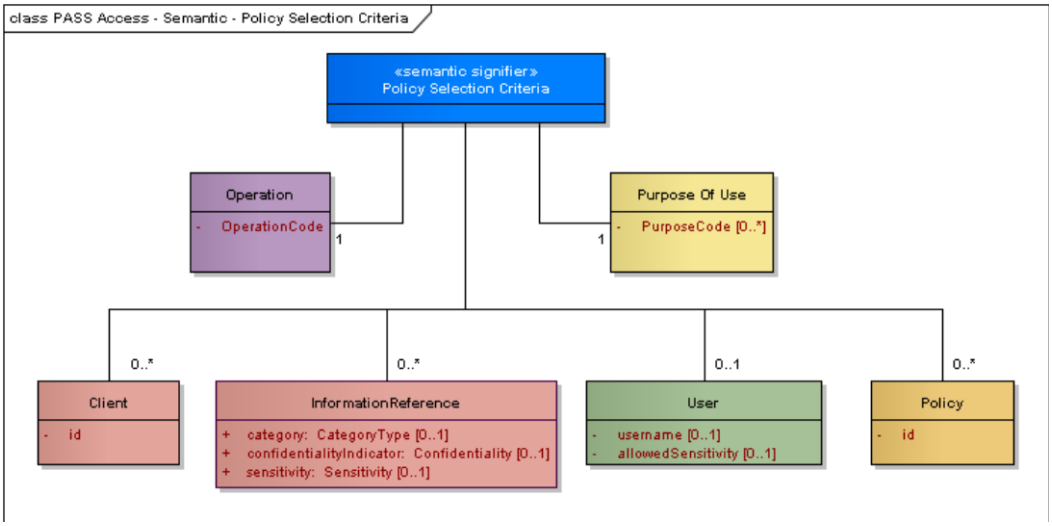

Figure 13: Policy Selection Criteria

Details of the business concepts and attributes illustrated above are as follows:

Table 6: Details of Policy Selection Criteria

Concept	Attribute	Description
Operation	OperationCode	This is the coded concept from the HL7 V3 RBAC Constraint Catalogue. Mandatory.
Purpose of Use	purposeCode	Purpose of Use identified for the collection, use, or disclosure of information. Mandatory.
Client	Id	A unique Client identifier, usually used to identify privacy policies or consent directives specific to that identifier. In order to support distributed policy stores, some federation mechanism will have to be implemented in order to map identities. Optional.

Concept	Attribute	Description
Information Reference	Category	Information category. Mandatory
Information Reference	confidentialiyIndicator	The confidentiality indicator is a coded attribute that assigns access controls on health records based on the information or type of access.[12] Optional
Information Reference	Sensitivity	Coded attribute that describes the sensitivity of a user or information artifact. [13] Optional.
User	Username	The login identifier associated with a person using an information system used to access IIHI.[14]
User	allowedSensitivity	Coded attribute that describes the sensitivity level of the IIHI that the user may access or use.[15]
Policy	Id	The unique identifier of the policy being requested. The likely scenario where this would be populated is when a currently-executing policy references an external policy. Optional.

4.4.3 Attribute Selector (Informative)

Purpose

These name/value pairs are specific attributes associated with each of Client, Requestor, or Resource entities. A generic request/response semantic structure allows for a flexible and extensible set of attributes as shown in Figure 14, below.

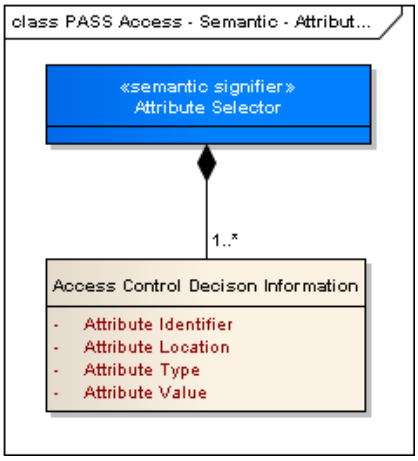

Figure 14:Attribute Requisitioning and Provisioning

This semantic signifier will be constrained by the information models provided by the Composite Privacy DAM, and the Security DAM.

[12] Source: Security Domain Analysis Model – Informative Ballot – January 2010
[13] Source: Security Domain Analysis Model – Informative Ballot – January 2010
[14] Source: Security Domain Analysis Model – Informative Ballot – January 2010
[15] Source: Security Domain Analysis Model – Informative Ballot – January 2010

4.4.4 Privacy Policy and Consent Directive

Purpose

The Privacy Policy is the executable policy that is selected and evaluated to provide access control decisions in conjunction with Security Policies. A Consent Directive is a Client-specific instance of a Privacy Policy.

Privacy Policies and Consent Directives are described in the Composite Privacy DAM (DSTU) – September 2009 and can be referenced in the Information Viewpoint section of the Composite Privacy DAM document.

4.4.5 Access Control Decision

Purpose

The Access Control Decision encapsulates the result of the access control request evaluation process, providing the decision along with any obligations that the applicable policy requires.

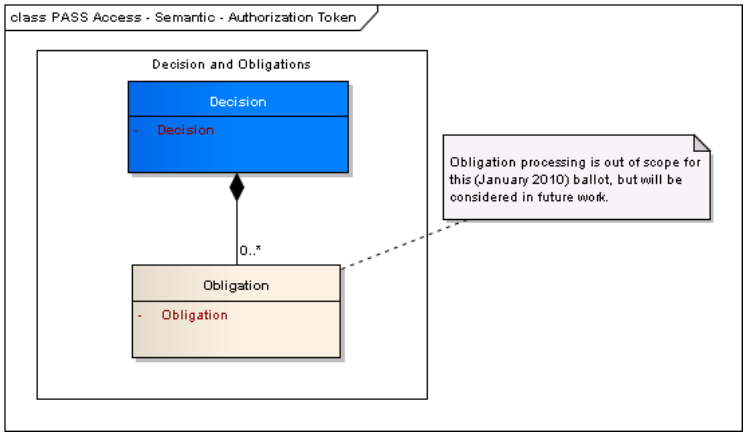

Figure 15: Policy Decision and Obligations

Details of the business concepts and attributes illustrated above are as follows:

Table 7: Details of Policy Decision and Obligations

Concept	Attribute	Description
Decision	Decision	A coded value indicating the decision that resulted from the evaluation of policy(ies) applicable to the request.
Obligation	Obligation	Coded value that describes technical or business obligations that are required to accompany the decision. Obligations are completely driven by policy. Optional

4.4.6 Policy Management Request

Purpose

The Policy Management Request encapsulates the lifecycle state transition events and associated information components for a Policy. Policy states are described in the Doman Analysis Models for both Composite Privacy (DSTU – September 2009), and Security (DSTU Ballot – January 2010).

In the Figure, Policy is shown as a generalization of both Privacy and Security policies as described in their respective DAMs. Please refer to those DAMs for detailed semantic information.

The following table describes the concepts and attributes from Figure 16, below.

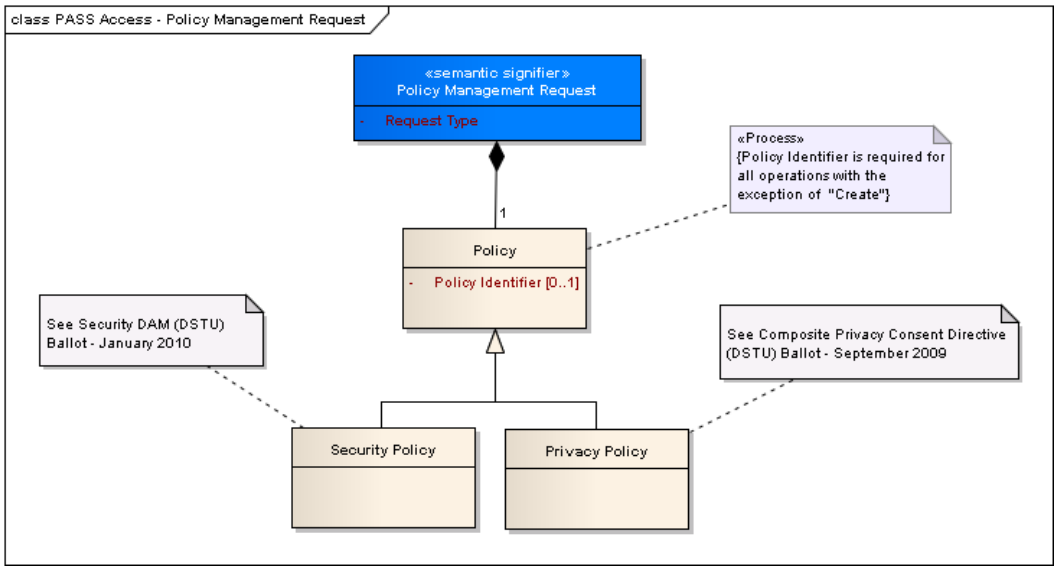

Figure 16: Policy Management Request

Table 8: Details of Policy Management Request

Concept	Attribute	Description
Policy Management Request	Request Type	A coded value indicating the operation that is to be performed on the accompanying policy. Mandatory.
Policy	Policy Identifier	A unique identifier for the policy. Mandatory except when the request type indicates that a new policy is to be created.

4.4.7 Policy Management Response

Purpose

The Policy Management Response encapsulates the results of an associated request for a lifecycle change a Policy. Policy states are described in the Doman Analysis Models for both Composite Privacy (DSTU – September 2009), and Security (DSTU Ballot – January 2010).

Consent Management provides the means to deal with Client privacy policies received from the outside, reflecting input from a Service Consumer, another Service Provider or from a Personal Health Record. Such policies are permitted but may require additional scrutiny and Privacy Management oversight in order to determine Service provider acceptance or agreement prior to placing in the directory of Privacy Policies.

The following table describes the concepts and attributes from Figure 17, below.

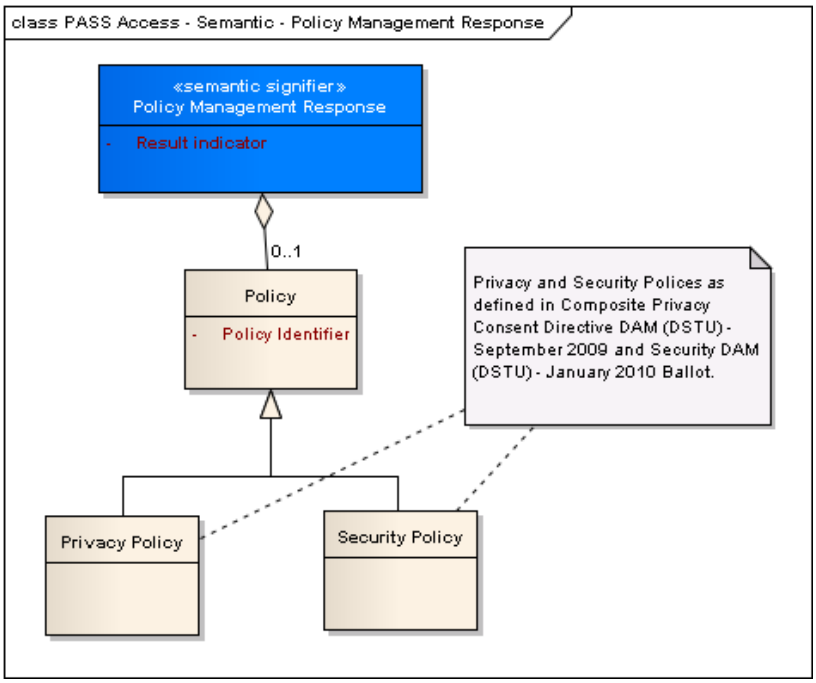

Figure 17: Policy Management Response

Table 9: Details of Policy Management Response

Concept	Attribute	Description
Policy Management Response	Result Indicator	A coded value indicating the result of the operation that was requested. Mandatory.
Policy	Policy Identifier	A unique identifier for the policy. Mandatory when Policy is present.

4.5 Dynamic Model

See PASS Access Control Release 1 dated January 2017

5 COMPUTATIONAL VIEWPOINT

5.1 Overview

A computational viewpoint on an SAEAF/RM-ODP system and its environment is a specification that enables distribution of the functional behavior of the system into service components which interact at interfaces. In the computational viewpoint, applications and business process realizations consist of configurations of interacting service components reflecting business roles participating in service collaborations.

The computation viewpoint is defined by a series of capabilities executed within the scope of an overarching set of high-level trust activities including:

Define the Federated Domain. Define the Federated Domain components including users, data, and policy contexts.

Derive (Negotiate) Federated Domain Basic Policies (Trust Proposal). Domain policies include consideration of the entire complex of legal, ethical, social, organizational, psychological, functional, and technical rules for ensuring trustworthiness of health information systems. [ISO 22600-2]. For the purposes of trust negotiation, trust rules are fully included in and defined by Basic policies. Run-time access-control focused aspects of Meta and Composite policy needed for access-control purposes do not apply and come into play only at the time authorizing a specific information request. Accordingly, this Trust Framework assumes Trust Policy is defined by Federated Domain Basic policy.[16]

By way of example, Federated Domain legal policy may require that the Initiator assert that they are a signatory to a Data Use Agreement applicable to a specific healthcare law. At run-time, such information would be provided as ADI for evaluation by an access-control service. If the ADI were not provided, then under the provisions of the Trust Contract access could be denied.

Execute the Trust Contract. Trust Polices establishing trust involve incorporating Basic policy aspects are included in a Contract signed by Domain Authorities. Authorities may assert an existing Trust Contract or derive (negotiate) a new Trust Contract as needed to describe the conditions under which information exchange is to occur. Trust is established when partners to an information exchange have agreed to the conditions of the exchange by executing and applying an (electronic) signature to a trust contract. This Contract should be considered legally binding.

Out of scope of Trust Framework but in scope of access-control:

Submit Information Request. Following establishment of trust, the process whereby an Initiator may make an information request from a Resource (under an established Trust Contract).

- **Initiate Information Exchange**. The process of adjudicating information request-related access control decision information in order to make an access

[16] We distinguish between policies needed to establish a general trust contract and those policies used to enforce access control. Run-time Access control policies include all of Basic, Meta and Composite policies. On the other hand, Domain policy and Contract policy is concerned primarily with Basic policy, the run time aspects of Meta and Composite being specific to a particular request rather than information exchange in general. That said, the distinction is not absolute and includes the possibility that Federated Domains could be defined so as to include Basic, Meta and Composite policy.

control decision, in the context of an established Trust Policy, including access control decisions and provision of response and obligations.

5.2 Capabilities

This section describes each of the behaviors that have been identified from the requirements. The attributes of Accountability Type, Role, and Dependencies act to provide input to determining what collaborations may be required to ensure that any contract associated with the capability is fulfilled.

5.2.1 Create Trust Proposal

Table 10: Create Trust Proposal

Name	**Create Trust Proposal**
Description	Initiates a proposal to negotiate/establish a trust relationship in support of information exchange.
Accountability Type	Authorization
Role	Domain Trust Service (Submitter of new or modified trust proposals)
Obligations	Trust proposals must be signed with certificates that chain to trusted authorities
Community	Indirectly, all other members of the community.
Prohibitions	None or N/A
Dependencies	None
Precondition	Structural, semantic and syntactic interoperability
Constraints	None or N/A
Postconditions	The Trust Proposal has been received by the recipient.
Exception Conditions	The Trust Proposal is incomplete and requires additional information.
Relationship to Levels of Conformance	Contains all policy ADI and policy assertion elements needed to initiate policy negotiation.

5.2.2 Review Trust Proposal

Table 11: Review Trust Proposal

Name	**Review Trust Proposal**
Description	Initiates a process to derive a set of common policies based upon the ADI and asserted policy conformance of the policy proposal as received including relevant Domain policy.
Accountability Type	Authorization

Role	Domain Trust Service (Submitter of new or modified trust proposals)
Community	Indirectly, all other members of the community.
Prohibitions	None or N/A
Dependencies	None
Precondition	Structural, semantic and syntactic interoperability
Constraints	None or N/A
Postconditions	The Trust Proposal has been received and forwarded as necessary to External Policy Management Services and Trustworthiness Assessment Services.
Exception Conditions	No applicable policy exists for negotiation purposes.
Relationship to levels of conformance	Trust Proposal

5.2.3 Derive Set of Common Policies

Table 12: Derive Set of Common Policies

Name	**Derive Set of Common Policies**
Description	Accepts policy information from Trust Proposal, Trust and External Policy Management Service in order to derive (negotiate) the set of common, domain-specific security and privacy policies required for trustworthy co-operation between collaborating domains
Accountability Type	Authorization
Role	Policy Bridging Service
Obligations	To evaluate policies applicable to the request and the information source and render common, domain specific policy set.
Community	Used by Trust Services to establish a legally binding Trust Contract between requestors and providers of protected information.
Prohibitions	None or N/A
Dependencies	External Policy Management Service
Preconditions	Make Trust Proposal
Constraints	Must use verifying sources consistent with degree of trust.
Postconditions	The initial Trust Proposal is accepted, the initial Trust Proposal is modified with policies required by the Target domain.
Exception Conditions	No applicable policy exists for negotiation purposes.
Relationship to levels of conformance	Trust Proposal

5.2.4 Assess Partner Trustworthiness (Optional)

Table 13: Assess Partner Trustworthiness (Optional)

Name	**Assess Partner Trustworthiness (Optional)**
Description	Adaptively evaluates events outside of the proposals or contract (e.g. Trustworthiness Assessment Service assessments that have the effect of holding in abeyance execution or continuing execution of the contract.
Accountability Type	Policy
Role	Trustworthiness Assessment Service
Obligations	Parties accept and honor as legally-binding contract
Community	Domain Trust Service
Prohibitions	None
Dependencies	None.
Preconditions	None
Constraints	None
Postconditions	Trustworthiness Assessment Service assessments are created that may affect execution or continuing execution of the contract or non-acceptance of a Trust Proposal.
Exception Conditions	None or N/A
Relationship to levels of conformance	None. Adaptive and changeable with changes in conditions.

5.2.5 Discover External Policies

Table 14: Discover External Policies

Name	**Discover External Policies**
Description	Accepts a request to return Trust Proposal relevant access control decision attributes and assertions.
Accountability Type	Trust validation
Role	External Policy Management Service
Obligations	Provide trustworthy source of verifiable trust assertions.
Community	Used by Policy Bridging Service
Prohibitions	None or N/A
Dependencies	Must be electronically discoverable
Preconditions	None
Constraints	None

Postconditions	The requested policy attribute values have been returned
Exception Conditions	One or more policy attribute identifiers are unknown. One or more policy attribute values are unavailable.
Relationship to levels of conformance	None

5.2.6 Review Trust Counter-Proposal

Table 15: Review Trust Counter-Proposal

Name	**Create Trust Counter Proposal**
Description	Creates Counter-Proposal to an existing Counter Trust Proposal
Accountability Type	Policy
Role	Domain Trust Service
Obligations	None
Community	Used by requester and information source (Target)
Prohibitions	None
Dependencies	Existing Trust/Counter-proposal must exist
Preconditions	Knowledge of Target policies if available
Constraints	None or N/A
Postconditions	The parties have successfully negotiated a Contract or failed to.
Exception Conditions	Policy exceptions exist that prevent mutual acceptance of Contract terms.
Relationship to levels of conformance	None

5.2.7 Create Trust Counter Proposal

Table 16: Create Trust Counter Proposal

Name	**Review Trust Counter-Proposal**
Description	Submits alternative conditions in response to an existing Trust Proposal
Accountability Type	Trust
Role	Domain Trust Service
Obligations	Counter-proposal must be acceptable to originator and signed.
Community	Domain Trust Services
Prohibitions	Must not be used for the purpose of excluding exchange (information blocking)
Dependencies	Partners response
Precondition	There is an existing Proposal submitted
Constraints	Must be relevant to the purpose of the original Trust Proposal
Postconditions	The Counter-Proposal has been accepted and signed by all parties (Contract established). Information exchange can proceed.

Exception Conditions	Partner exceptions conditions are discovered through continuous assessment.
Relationship to levels of conformance	None or N/A

5.2.8 Accept Trust Proposal/Counter-Proposal

Table 17: Accept Trust Proposal/Counter Proposal

Name	**Accept Trust Proposal/Counter Proposal**
Description	Acceptance of a Trust Proposal or Counter-Proposal
Accountability Type	Policy
Role	Domain Trust Service
Obligations	Parties accept and honor as legally-binding contract
Community	Domain Trust Services
Prohibitions	None or N/A
Dependencies	Proposal exists, Review Counter-Proposal
Preconditions	None or N/A
Constraints	None or N/A
Postconditions	A machine-readable policy (contract) has been derived (negotiated)
Exception Conditions	Events outside of the contract (e.g. Trustworthiness Assessment Service assessments that have the effect of holding in abeyance execution or continuing execution of the contract.
Relationship to levels of conformance	None

5.3 Collaboration Analysis

This section discusses the interactions between services classified by roles

5.3.1 Federated Trustworthy Interoperability

See the HL7 Version 3 Standard: Privacy and Security Architecture Framework-Volume 2 Trust Framework for Federated Authorization Behavioral Model Release 1 for analysis of Federated Domain Model capabilities, policy federation, trustworthy interoperability, and Logical components and other collaboration analysis aspects.

A collaboration diagram follows which illustrates the collaborations necessary to complete the negotiations needed to establish a TF4FA Federated Trust Contract.

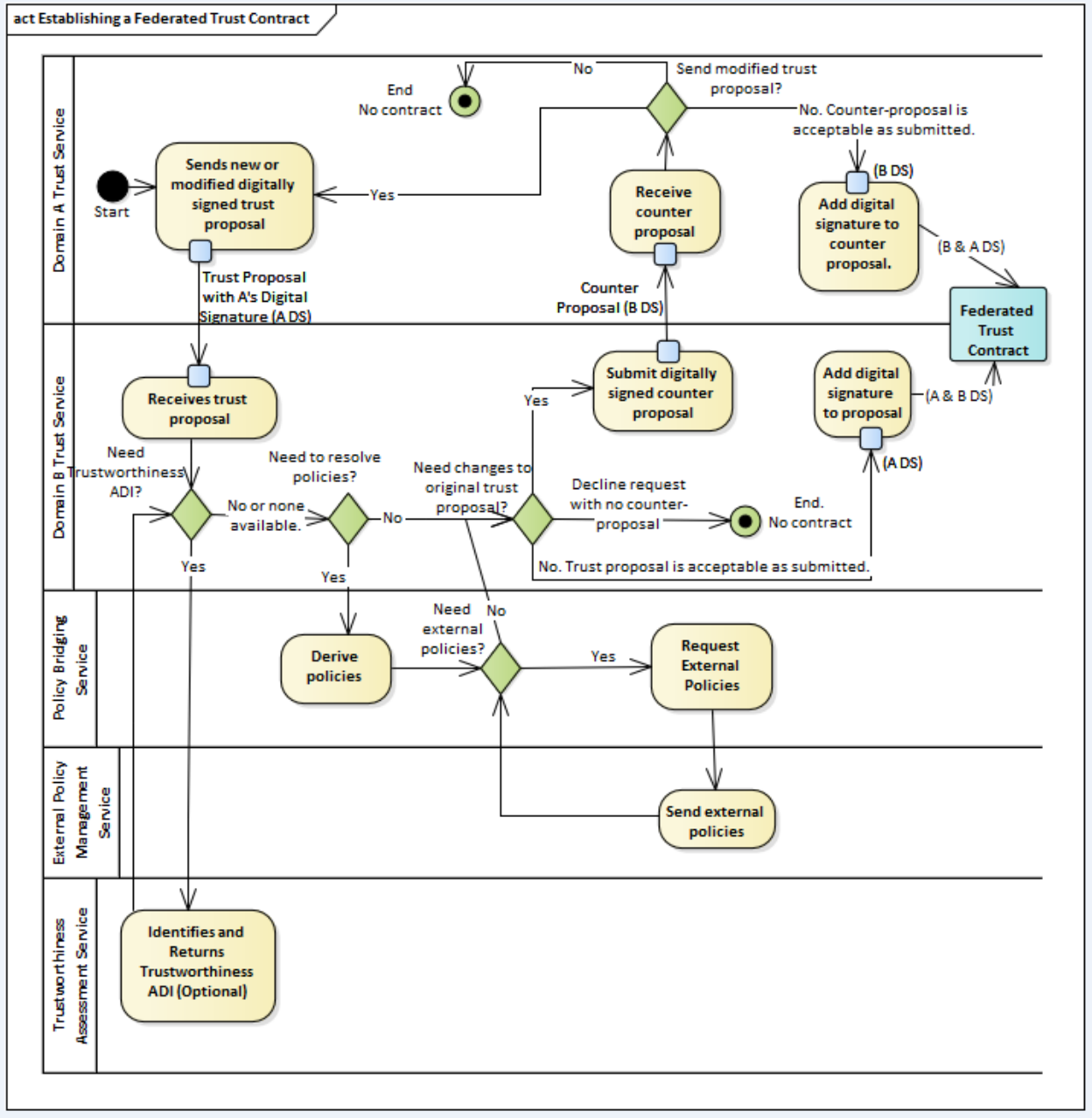

Figure 18: Capability Collaborations for Establish Federated Trust Contract

Note: This diagram assumes that Domain B is the owner of the data being requested. If Domain B in turn wants data from Domain A, then the roles for the Domain A and B Trust Services would be reversed.

1. The Domain A Trust Service submits a new or modified digitally signed trust proposal to the target
2. The Domain B Trust Service receives the trust proposal.
3. (Optional) The Domain B Trust Service gets trustworthiness ADI pertaining to Domain A from the Trustworthiness Assessment Service.

a. Note: The trustworthiness ADI is returned to the Trust Service and may be used to determine if Domain B is willing to continue the process or additional requirements could be added to a counter-proposal in order for a trust contract to be established.

4. The Domain B Trust Service determines if policies need to be resolved.
   a. If they do, the Policy Bridging Service:
      i. Determines if external policies are needed.
         1. If they are, then the Policy Bridging Service invokes the External Policy Management Service.
            a. The External Policy Management Service returns all needed external policies.
         2. If no external policies are needed, or all external policies have been acquired, the Policy Bridging Service returns the results of the policy derivation to the Domain B Trust Service.
5. The Domain B Trust Service determines if changes are needed to the original trust proposal. There are three possibilities:
   a. No changes are needed. The trust proposal is acceptable as submitted. Since Domain A Trust Service's original digital signature is intact, the Domain B Trust Service adds its digital signature and the trust proposal becomes the final Federated Trust Contract.
   b. Request is denied, and the transaction is terminated with no contract.
   c. Changes are needed. A digitally-signed counter proposal is created and sent to the initiator.
6. If a digitally signed counter proposal is submitted, the Domain A Trust Service may:
   a. Accept the counter proposal as submitted. Since the Domain B Trust Service's original digital signature is intact, Domain A Trust Service adds its digital signature and the counter proposal becomes the final Federated Trust Contract.
   b. Decide to drop the request and end the transaction with no contract.
   c. Make changes to the Domain B Trust Service counter proposal and create a modified, digitally signed, trust proposal.
      i. This puts the process back to step 1 where it continues until a Federated Trust Contract has been established or the transaction is terminated by either the Domain A or B Trust Service.

5.3.2 Policy Management

The Policy Manager role fulfills the capabilities associated with the lifecycle and provisioning of executable privacy and security policies. Policy classes that inform attributes of privacy and security policies are contained in the Composite Privacy DAM (DSTU) – Sept 2009, and Security DAM – January 2010 (Informative Ballot).

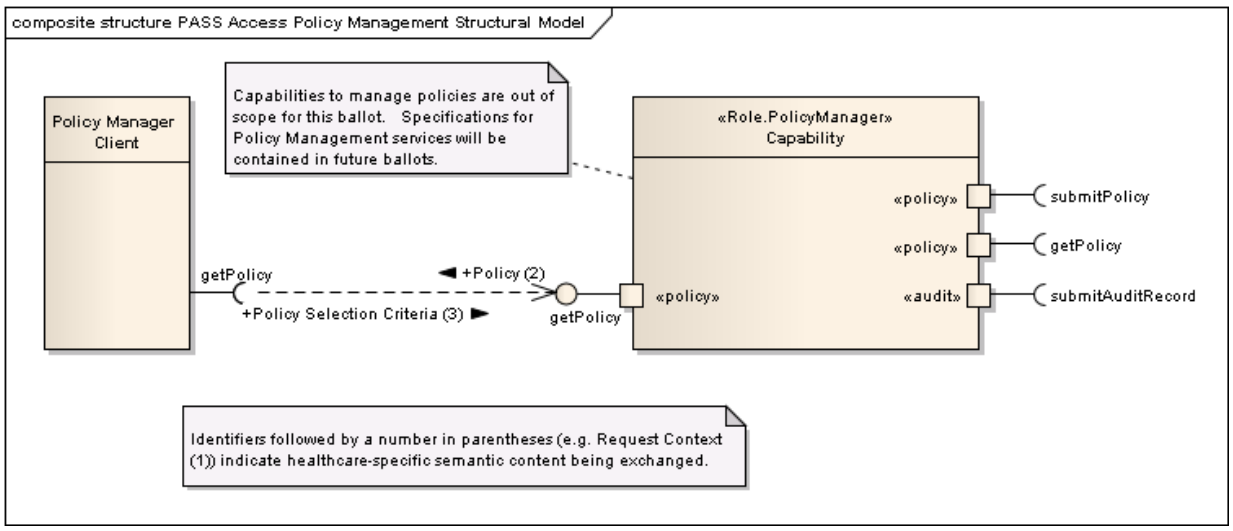

Figure 19: Policy Management Roles and Capabilities

5.4 Conformance

This section identifies those contracts and profiles that will be necessary for working interoperability.

In the computational viewpoint, there exists a reference point at any interface of any service component. A conformance statement is a statement that identifies conformance points of a specification and the behavior which must be satisfied at these points. Each reference point can become a conformance point based on conformance assertions made by referencing specifications in other viewpoints or less abstract specifications at a platform independent or platform specific level.

A contract can apply at a given reference point in a system. Conformance relies on evaluating the interactions between roles against their contractual obligations. In that case, it specifies the functional behavior which can be expected at the reference point.

Conceptual-level conformance statements will only occur in standards which are intended to constrain some feature of a real implementation, so that there exists, in principle, the possibility of testing. The following contract specifications and conformance profiles constitute conceptual conformance statements.

This document leverages the conformance contracts and conformance profiles contained in HL7 Version 3 Standard: Privacy, Access and Security Services (PASS) Access Control, Release 1 January 2017

See also HL7 Version 3 Standard: Privacy and Security Architecture Framework – Volume 2 Trust Framework for Federated Authorization Behavioral Model, Release 1, Conformance statements and assert Technical Framework Conformance Statement.

Further healthcare-specificity stems from the combination of cross-industry access control standards with healthcare-specific semantics.

6 ENGINEERING VIEWPOINT

This section identifies the infrastructure that is required to support functional distribution of an ODP system[17] at the conceptual level.

6.3 ODP Functions

The ODP Functions are specified by ISO/IEC 10746-3 Open Distributed Processing – Reference Model Architecture and are intended to provide broad categories of functions to be considered. At the conceptual level, the majority of these functions would not necessarily be filled.

6.3.1 Physical Distribution Functions

N/A

6.3.2 Communication Functions

N/A

6.3.3 Processing Functions

N/A

6.3.4 Storage Functions

N/A

6.4 Engineering Roles

None identified.

[17] ISO/IEC 10746-3 Open Distributed Processing – Reference Model Architecture

Appendix A: Glossary of Terms

The following table identifies terms used in this document that are specific to the subject domain.

Term	Definition
Access Control	A means of ensuring that the resources of a data processing system can be accessed only by authorized entities in authorized ways ISO/IEC 2382-8, definition 08.04.01
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 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)	ACI is 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/IEC 10181-3] Any information used for access control purposes, including contextual information. ISO TS 22600-1:2006 Contextual information might include source IP address, encryption strength, the type of operation being requested, time of day, etc. Portions of ACI 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". [XACML]
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 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]

Term	Definition
Access Decision Information (ADI)	Policy attribute values.

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]
Attribute	Characteristic of an initiator, resource, action or environment that may be referenced in a predicate or target. [XACML] A claim of a named quality or characteristic inherent in or ascribed to someone or something. [NISTR 8112] 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] 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 Metadata	Data providing information about the context and structure of an attribute. See metadata. [NISTR 8112]
Authorization	A process of granting rights, which includes the granting of access rights ISO TS 22600-1:2006
Authorization	The granting of rights, which includes the granting of access based on access rights. [ISO 7498-2] The granting of privileges, which includes the granting of privileges to access data and functions. [ISO 22600-2 – modified from ISO 7498-2] 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]
Term	**Definition**
Authorization/attribute access control	Access control based on values of access control information
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 "plan or course of action adopted for providing computer security."

Classification	Security label metadata that specifies the labeled resource's level of confidentiality. [HL7 PASS SLS] 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] Permission granted to an individual to access data or information at or below a particular security level. [ISO/IEC 2382-8:1998]
Clearance Attribute	The clearance attribute is used to define the authorizations granted a specific user or application entity. [ITU X.841]
Confidentiality	Use definition from HCS
Contextual Information	Information about or derived from the context in which an access request is made (e.g. time of day). [ISO 10181-3]
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] See also Security Domain.
Domain Characterization	A domain is characterized by a domain identifier, domain name, domain authority, and domain qualifier (ISO 22600-2:2006).
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]
Emergency access	Access permitted by policy when an emergency condition exists
Environment	The set of attributes that are relevant to an authorization decision and are independent of a particular subject, resource or action. [XACML]
Environmental variables	Those 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 TS 22600-3:2006
Term	**Definition**
Federated Policy Domain	In a federation, each domain retains most of its authority while agreeing to afford the other limited rights. The federation agreement records: The rights given to both sides, such as the kind of access allowed. The trust each has in the other. 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] 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 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. The choice of mechanisms, in turn, is dependent upon trust relationships between the domains. [WS-Federation]
Functional (Requirement)	"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. (confirm definition [HIMSS])
Handling Instructions (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] 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 an HCS conformant security label. [HL7 HCS]
Individually Identifiable Health Information	Health Information that contains or can be reconstituted to refer to a specific, identifiable individual.

Term	Definition
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 it can provide sharable, stable, and organized structure of information requirements for the domain context [Info Model]. 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]
Integration	The act of bringing together data and/or capabilities from two or more independent applications, within the same enterprise or across multiple enterprises
Inter-domain communication and cooperation	Interoperability between domains is called an inter-domain communication and co-operation. [ISO 22600-1] See also Security Domain. See also Interoperability.
Multidomain Information Object (aka Compound Domain)	A collection of objects from different security domains perceived by users as a single information object. In compound security domains, additional policies are written that apply to the newly created multidomain information objects. The multidomain information security policy states 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]
Organizational Policy	Class of policy used to represent an organization that may be issuing privacy and/or security policies. [HL7 DAM]

Term	Definition
Policy	A set of legal, political, organizational, functional and technical obligations for communication and cooperation [ISO TS 22600-1:2006] The rules and criteria that constrain activities of the objects to make the domain secure. [OMG SEC] 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] 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] 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 Administration Point (PAP)	The system entity that creates a policy or policy set. OASIS XACML
Policy Bridging	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 Decision Point (PDP)	A system entity that makes authorization decisions for itself or for other system entities that request such decisions. OASIS XACML
Policy Enforcement Point (PEP)	A system entity that requests and subsequently enforces authorization decisions. OASIS XACML
Policy Information Point (PIP)	The system entity that acts as a source of attribute values. OASIS 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] Provenance of a resource is a record that describes entities and processes involved in producing and delivering or otherwise influencing that 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]

Term	Definition
Purpose of use	Security label metadata that indicates the stated intent for access to privacy data. [HL7 PASS ACS] 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 v3 Vocabulary] 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 v3 Vocabulary] Purpose of use is an attribute that refers to the broader context in which an access takes place and captures the overall goal the requester tries to reach by accessing the data. The purpose is usually revealed in the answer to questions such as "how is the requester going to use this data item?" and "what is the requester going to use the data for?" 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] Security label metadata that indicates the stated intent for access to privacy data. [HL7 PASS ACS]
Resource	An entity to which access may be attempted. [ISO 10181-3]
RIM	Add definition
Role, functional	Named set of permissions controlling fine-grained accesses within a resource such as an application. 22600? ANSI 359
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 Domain	A set of subjects, their information objects, and a common security policy (NIST Special Publication 800-33).

Term	Definition
Security Domain	A set of subjects, their information objects, and a common security policy. [NIST SP 800-33] Security Domain Attributes: Within a security domain, all information objects exist at the same level of sensitivity [ASTM E2595]. Note: this is synonymous with the "confidentiality classification" found in [HL7 HCS]. Members of a domain may have different security attributes, such as read, write, or execute permissions on information objects. [ASTM E2595] Security domains are not bound by systems or networks of systems. [ASTM E2595] A security domain's objects may reside in multiple systems. [ASTM E2595] 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] A collection of users and systems subject to a common security policy. [ITU X.841] 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] A single unit of security administration or trust. [WS-Federation]

Term	Definition
Security Policy	The complex of legal, ethical, social, organizational, psychological, functional, and technical rules for ensuring trustworthiness of health information systems. [ISO 22600-2] 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 security policy domain is a set of objects to which a security policy applies for a set of security related activities and is administered by a security authority. The objects are the domain members. Policy represents the rules and criteria that constrain activities of the objects to make the domain secure. (OMG Security Services Specification (OMG SEC))
Security policy enforcement	Security policy enforcement deals with ensuring that users attempting to access system functions and data possess attributes (such as privileges granted and provisioned in security and privacy management) equal to or greater than that required for the access
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	(use definition from HCS)
Subject of Care	One or more persons scheduled to receive, receiving, or having received a health service. [ISO 27799]
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]
Term	**Definition**

Target	An entity to which access may be attempted. [ISO 10181-3] The set of decision requests, identified by definitions for resource, subject and action that a rule, policy, or policy set is intended to evaluate.
Trust	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 principals and/or digital identities. In the general sense, trust derives from some relationship (typically a business or organizational relationship) between the entities. [WS-Federation] 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. 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 Context	The environmental, legal, social, and technical components of a Federated Domain.
Trust Contract	The mutually agreed upon technical, social and operational context under which information exchange may occur. Check 22600-3 Sets of rules followed by the parties involved for achieving interoperability. [Based on ISO 22600-1]
Trust Policy	Trust policy elements used to derive (negotiate) the common agreed upon policies of a trust contract. Pre-contract policy element. A list of capabilities that an entity can assert in establishing a trust contract. 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. Trust security metadata are observation made about aspects of trust applicable to an IT resource (data, information object, service, or system capability). 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 IEC 10181-1 and NIST SP 800-63-2]
Term	**Definition**

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] 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]
User	A consumer of the services offered by an RP. [NISTIR 8149]

Appendix B: Acronyms

ACL: Access Control List
ACI: Access Control Information
ADI: Access Control Decision Information
ACS: Access Control List
DAM: Domain Analysis Mode
DS: Digital Signature
ED: Emergency Department
EMR: Electronic Medical Record
HCS: Healthcare Classification System
IIHI: Individually Identifiable Health Information
LCD: Lowest Common Denominator
OID: Object Identifier
PDP: Policy Decision Point
PEP: Policy Enforcement Point
PHR: Personal Health Record
PKI: Public Key Infrastructure
ReBAC: Relationship-Based Access Control
RBAC: Role-Based Access Control
RM-ODP: Reference Model of Open Distributed Processing
SAEAF: Services Aware Enterprise Architecture Framework
TF4FA: Trust Framework for Federated Authorization

Appendix C: Referenced Standards

The following standards are referenced and provide foundational components for this work:

[ASTM E1986]	(add information)
[ASTM E2595]	(add information)
[GTRI]	(add information)
[HIMSS]	(add information)
[HL7 DAM]	HL7 Composite Security and Privacy Domain Analysis Model, May 2010 (Publication Ongoing)
[HL7 PASS ACS]	HL7 Version 3 Standard: Privacy, Access and Security Services (PASS) Access Control, Release 1, January 2017
[HL7 PASS ACS]	HL7 Version 3 Standard: Privacy, Access and Security Services (PASS) Access Control, Release 1, January 2017
[HL7-HCS-VOCAB]	HL7 Privacy and Security Vocabulary Tables (August 29, 2012) http://gforge.hl7.org/gf/download/docmanfileversion/6897/9534/HL7PrivacyandSecurityVocabularyTables.docx
[ISO 7498]	(add information)
[ISO 10181-1]	ISO/IEC 10181-1:1996-Information technology -- Open Systems Interconnection -- Security frameworks for open systems: Overview
[ISO 10181-3]	ISO/IEC 10181-3:1996 – Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework – Access Enforcement Function “intercept” modeling
[ISO 22600]	ISO 22600 series – Policy Management and Access Control – Basic Access Control Model
[ISO 27799]	(add information)
[ITU X.800]	(add information)
[ITU X.841]	(add information)
[NIST SP800-33]	(add information)
[NIST-SP800-63]	

[NIST SP 800-162]	(add information)
[NISTR 8112]	(add information)
[OASIS XACML]	OASIS XACML 2.0 Specification – Terminology
[OMG SEC]	(add information)
[PONDER]	Ponder: A Language for Specifying Security and Management Policies for Distributed Systems, Version 2.3, 20 October 2000 https://www.hl7.org/documentcenter/public_temp_AFF26CFD-1C23-BA17-0C56CE0E3FAEB5EA/wg/mnm/hdf/PonderSpec.pdf
[SAEAF]	Service Aware Enterprise Architecture Framework (add definition)
[W3C Provenance]	(add information0
[WS-Federation]	(add information)
XSPA	(add information); Cross-Enterprise Security & Privacy Authorization

