2013-10-02

The “Modular” Federated Credential and Identity Model

A General Model for Federated Credential and Identity Frameworks

Version 05 ***DISCUSSION DRAFT***

A Work Product of the Kantara Initiative Identity Assurance Working Group

Editor: Andrew HughesAndrewHughes3000@gmail.com

Table of Contents

Andrew Hughes 11/13/13 9:45 AM
Deleted: 1

Andrew Hughes 11/13/13 9:45 AM
Deleted: 2

Document Management

Contributors

Editor:	Andrew Hughes AndrewHughes3000@gmail.com
Contributors:	Ken Dagg, Scott Shorter, Myisha Frasier-McElveen, Cathy Tilton
Reviewers	Kantara Initiative Identity Assurance Working Group

Document Control

Date	Version	Description
2013-09-17	V04	Discussion Draft with core elements mostly defined and enumerated.
2013-10-02	V05	Additional details added.

Table of Figures

Overview

NOTE TO REVIEWERS: This is a first discussion draft version (05). Some sections are incomplete or missing. The intent of distributing this discussion draft is to solicit feedback from IAWG on the structure of the document, the concept of data records being the focus of functions, and the function-role mappings. Please focus on the content only at this time, and please avoid minor grammatical corrections.

Synopsis

Introductory text goes here…

Objectives of the Paper

- To concisely define the Roles, Functions and Services found in Federated Credential & Identity models which are compatible with the Kantara Identity Assurance Framework
- To specify typical arrangements of Organization to Role found in Kantara’s target audience of Federated Credential & Identity Service providers
- To specify, if possible, specific criteria in the Kantara Service Assessment Criteria v3.0 document that might span more than one archetypical Organization-Role association

Anticipated Outcomes

- The anticipated outcome of this work will be a report that sets out archetypical Organization and Role assignments in Credential & Identity Federations that are compatible with the Kantara IAF Trust Framework.
- The report will be usable by Trust Framework Architects as a baseline for determination of divisions of responsibility and Role in the Kantara IAF
- In future phases of the work, the report could be used to define and establish alternative arrangements for Kantara Trustmarks, although this is not the primary purpose of the work.
- The report will consider implications and impacts on the Assessment and Approval processes.

Rationale and Uses for Models

If designed well, a model can be used to investigate different arrangements in a solution. If the model is made Modular, services and functions can be swapped in and out as needed to meet new requirements; or insourced or outsourced to meet resource allocation needs.

In this paper, alternative function and role arrangements will be explored to examine implemented credential and identity solutions and patterns. Each pattern was developed and deployed to meet requirements.

A Functional Model contains the set of unique Functions present in a solution that are related to delivery of directly relevant services. This contrasts to the Non-Functional Model, which includes functions relevant to an IT system delivering the Functions and Services.

A Relationship Model describes how organizations, roles, functions and services relate. It describes accountabilities and hand-off points. It describes information types flowing between the parties.

Time sequences are core to Process and Services definitions. In some cases, modifying the time sequence of invoking functions or services is all that is needed to describe an alternate approach to solution.

Implications for Kantara Identity Assurance Framework

The next step after this model is finalized is to map the Service Assessment Criteria to the functions and roles of the model.

It may be then possible to reconfigure the Assurance Assessment Scheme to allow for sub-assessments of Role sets and Function sets. There may be a possibility of new Approval types to arise from the new arrangements.

Overall approach

- The current work effort will elaborate on the ‘Decoupled Binding Model’ paper submitted to the IAWG in Fall 2012
- IAF v3.0 will be analyzed for criteria alignment and implied Roles
- The IAF v3.0 to NIST SP800-63-2 mapping work will be included in the analysis to ensure that this work aligns with the next version of IAF
- A subgroup of interested participants from the IAWG will meet regularly to discuss the subject and assist the document Editor to make progress

Prior publications, related work and basis documents

The “Decoupled Binding Model” draft paper submitted to the IAWG in Fall 2012. Located at KantaraInitiative.org

More Text needed here – should mention the GSA, NIST and IDESG parallel work

A word about words

In this paper, the term “Model” is used frequently. The sense intended for “Model” is a set of related diagrams, schematics, narratives and sequences that convey meaning about the workings of a system. A Model represents part of an overall design, and is based on requirements.

The Model is usually an instantiation of a General Model or Pattern. The General Model can be considered to be descriptive of a Class of Models; each Model being an instantiation.

The General Model and its class family therefore have similar operating rules, permitted relationships and core concepts. A General Model will exist for each conceptually distinct approach to solve a given problem.

In this paper, the term “General Model” may replace the term “Modular Federated Credential and Identity Model”.

Federated Credential and Identity Models

Evolution of the Paradigm

The paradigm and concepts of “Trusted Identity Frameworks” have emerged from the patterns and technologies of user account and authentication federation. In these federated access control patterns, one entity chooses to accept assertions made by another entity, based on pre-established agreements and common communication protocols. Typically, federated access control patterns have been used to accept user account authentication from one entity to enable access and authorization to another entity’s protected resources.

Early on, user accounts and their associated system profile information were considered to represent the Person in the system. This eventually led to the idea that the Person’s “Identity” in the real world was directly equivalent to the user account and profile in the system. The user account was “bound” to the real person using an authentication secret such as a password. Thus, by entering the password, it was assumed that the individual had “proved” that they had control of the account, and that it was the same person, the Subject, that had been issued the account in the first place. Of course, since the binding mechanism is very weak, nothing could actually be proven.

As access control patterns matured, the concepts of externalization of credential management and authentication matured as well. The owner of the protected resource was considered to rely on the credential and authentication provider, and was called the Relying Party. Due to the historical association between a person and their user account, the authentication provider became the Identity Provider. If the Identity Provider was also providing information along with authentication services, in certain contexts it became known as the Authoritative Party.

The separation of credential provisioning from resource access control and the reliance on external service providers for credentials, authentication and information attributes are hallmarks of federated access control patterns.

The Rationale for Modularity

The term “Modular” in this discussion paper refers to groups of related Service Assessment Criteria in the v3.0 of the Kantara IAF. The orientation is towards Functional groupings: Functions that an autonomous organization or sub-organization could reasonably be expected to provide.

In the Model, these Modular groupings (sections of the SAC) are equivalent to “Roles”. A Role is accountable for a group of Functions. The Roles in this Model are more finely grained than the modules defined in the current version of IAF.

Modules as they relate to Assessment Criteria

The Kantara Identity Assurance Framework and associated approval program use the concepts of Service Components and full Credential Service Providers. The Service Assessment Criteria are organized into three parts: Common Organizational, Identity Provider and Credential Manager.

Currently, there is no easy way to design and express different arrangements of criteria based on actual or planned implementations. If the implementation does not match the structure of the Service Assessment Criteria, then complex and onerous procedures must be undertaken to demonstrate coverage of all the criteria. This is a custom solution to the problem.

By using a standardized model such as the one described in this paper, a greater degree of flexibility is possible. Common terms and concepts can be used to describe implementation choices, thereby improving communication and speeding understanding.

The IAF and SAC Modules could be reorganized along the lines of the Roles. Such an arrangement could lead to new Approval types or more flexibility in which organization performs which functions.

By having finer-grained Roles, it may be possible to increase standardization along functional lines, thus making it easier to describe actual implementations in terms of the Service Assessment Criteria structures.

Issues With Credential, Identity and Federation Terminology

Several federated access control patterns have emerged, each with its own conceptual framework, context and terminology. Imprecise usage of terms among the patterns has led to an unfortunate confusion over terminology and understanding of capabilities. For example, many use the term Identity Provider or IdP to mean the entity that issues credentials, authenticates credentials and supplies information about the logged-in-user. Others use the same terms to mean the entity that holds an “Identity Record” with information related to an individual, and offering services of authorized release of that information to requesters.

It is important to understand that many terms used in the federated identity patterns have specific technical meanings that do not map well to their English language meanings.

Knowledgeable practitioners tend to use these labels interchangeably and expect others to understand their meaning based on the context that the label is used. However, confusion over the precise distinctions between roles, terms and services arises when non-technical people or those not deeply versed in electronic authentication concepts attempt to exchange information and ideas with others.

This paper will not describe the range of current patterns and technologies used for federated access control and federated information sharing.

The Modular Federated Credential and Identity Model

Key Concepts and Terms in the General Model

The General Model uses several key concepts:

- Information in storage is structured into *Records*
- Records contain Data and Data Sets required for the *Functions* and *Roles* associated with the Records
  - ***Assumption***: In this paper, Records are a concept, not a real-world data structure.
- Information being communicated is an *Assertion*
  - ***Assumption***: Assertions are not created ‘on the fly’. The asserted information is first retrieved from the Record or created and stored in a Record, then is asserted. In the case of ephemeral self-originated information, within this model it should be considered to be stored, even if it is not stored in a real implementation.
- A Data Set is related Information, often stored in a Record or transmitted in an Assertion
- An *Originator* ‘creates’ the first recorded instance of a particular data set
- An *Authoritative Source* is the Entity legally defined as authoritative over the data set.
  - The Authoritative Source may also be the data Originator
  - *Consider*: The attending physician is the Originator of birth facts; the Vital Statistics department is the Authoritative Source of some of those facts.
- A *Role* is accountable for a collection of Functions.
- *Functions* exist to act on Information.
  - *Data-related Functions and sub-functions include*: Collect Data Set; Consume Data Set; Transform Data Set; Link Data Set with other set or sets; Assert Data Set; Verify Data Set; Store Data Set; Search Data Set; Match Data Set; Encrypt Data Set; Decrypt Data Set; ‘Hash’[1] Data Set; Determine Uniqueness between Data Set and other Data Set.
  - *Entity or Object Functions and sub-functions include*: Generate identifiers; Obtain Information; Verify that information pertains to the Entity or Object; Validate that information is correct;
  - *Record management Functions and sub-functions include*: Create Record; Read Record; Update Record; Delete Record; Archive Record; Suspend Record; Transfer Record; Confirm Record Accuracy; Log Record Activity; Audit Record Activity; Confirm Security and Privacy Control Effectiveness.

Andrew Hughes 9/23/13 10:19 AM

Comment [1]: Need to include the cases where there are Originators that have no Legal basis for the Authority – ACH To ask Smeddinghoff – this is probably wrong – most departments have to get their information practices approved but they are not the “Legal Authority”

[1] A very loose use of the term ‘hash’. Intended to mean ‘create a value derived from the data set using cryptographic means which uniquely relates to the plaintext data set’

- There are currently several *Role Types*: *Managers, Validators, Brokers, Information Consumers*
  - A *Manager* role is one that is accountable for managing one or more Records.
    - Subject Record Manager, Token Manager, Credential Manager and Service Manager are examples
  - A *Validator* role is one that checks Information against Authoritative Sources and makes an assertion about it
  - A *Broker* role intermediates interactions between other roles, sometimes transforming information in the process.
  - An *Information Consumer* role consumes Assertions. Most of the roles have some element of information consumption, so this role may not be explicitly assigned in all cases.
- An *Entity* can be a Person, Non-Person Entity or Organization.
  - Entities can be assigned Roles, which confers accountability to perform Functions on Information. An Entity can be assigned to zero, one or many Roles.
- A *Subject* is the Entity referred to in a Record
  - ***Assumption***: A Record must have a Subject.
  - ***Assumption***: When ‘Assurance Level’ is used in reference to a Record, it is used to express the certainty that the Record’s Subject refers to the expected Entity. Lower Assurance Levels indicate less certainty. Higher Assurance Levels indicate greater certainty.

Andrew Hughes 9/23/13 10:33 AM
Comment [2]: Read Canadian standard re Assurance Level re accuracy, linkability, evidence etc. Also a definition of the 4 ALs

“Binding”, “Assurance Level” and Electronic Transactions

“Binding an Entity to a Token”, “Binding an Entity to a Subject Record” refers to the Token Manager Role or Identity Manager Role respectively creating records that contain a unique reference to the entity and token for the former, and the entity and Subject record for the latter.

The “Binding” action allows use of the Token to represent the Entity and the Subject Record to describe the Entity in electronic transactions.

Assurance Levels range from lower to higher, typically in discrete increments. “Higher” assurance levels are said to have ‘stronger’ bindings due to the increased process rigour and increased security, evidence and verification stringency requirements.

The Online Service Provider assesses risk related to the online transactions offered and determines what level of assurance for credentials is required. Due to the links contained within the various Records, a higher assurance level directly relates to the degree of confidence of the identity of the Entity about to engage in the transaction.

‘Real World’ Organizations

The general model uses Entities and Roles to describe action-taking participants.

In order to model a ‘real world’ implementation, the analyst must assign individuals, non-person entities and organizations to the appropriate Entities and Roles.

The specific name of the ‘real world’ participant is, of course, specific to the nomenclature of the implementation.

There are nuances to the terms in use in any given implementation, and using incorrect names is a major source of confusion. However, there are some commonly used names for federated identity implementations.

Table 1: Real World Entities and Organizations

Name	Description
Individual	Generally the Subject referred to in the Subject Record
Credential Service Provider	In the NIST SP800-63 sense: an organization that offers Credential Management services, Identity Proofing & Verification services, and Identity Provider services
Attribute Provider	The organizations that assert information about Subjects
Identity Provider[2]	The term Identity Provider has come to mean a specialized Attribute Provider which primarily asserts Identifying Information about Subjects.
Online Service Provider	The provider of online services. Since the Online Service Provider must rely on other organizations in order to make access control and account decisions, it is often referred to as the “Relying Party[3]”.

[2] The term “IdP” has too many conflated definitions to be used reliably. We recommend avoiding this shortened form when discussing federated credential and identity models. Reserve its use for specific implementations that can define their own specialized terminology.

[3] The term “Relying Party” is loosely used in the field and the clarity of its definition has degraded substantially. Reserve its use for specific implementations that can define their own specialized terminology.

Diagram of Roles, Functions and Records Relationships

The diagram shows the relationships between the components of the Modular Federated Credential and Identity Model. See the pages following for descriptions and details.

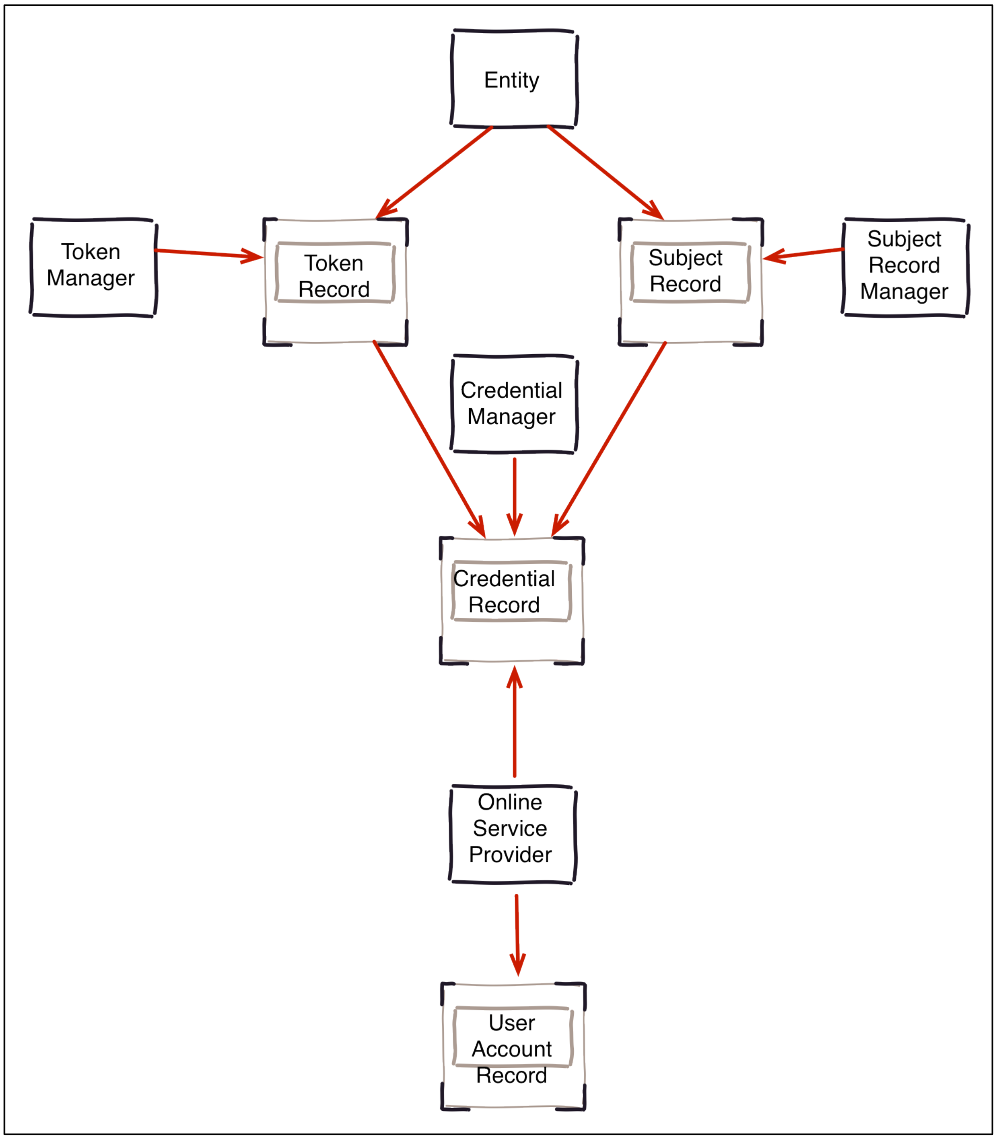

Figure 1 Diagram of Roles, Functions and Records Relationships

Records in the General Model

As noted above, Records are the focus of this General Model. The Records are comprised of Data Sets or Information; have specific Functions associated with them; and should be thought of as "data at rest" or "data in storage".

The record types at the core of this General Model are:

Table 2: Record Types And Their Data Sets

Record Type	Data Sets Stored & Examples
Subject Record	• *a.k.a. Identity Record; Attribute Record* • Identifiers that link the Entity to the Subject that the Subject Record pertains to • Information about the Subject • Subject Attribute Data • Subject Metadata • Process Metadata
Token Record	• Identifiers that link the Entity to the Token described in the Token Record • Information about the Token • Token Attribute Data • Token Metadata • Process Metadata
Credential Record	• *a.k.a. Token-Subject Link Record* • Identifiers that link the relevant Subject Record and Token Record • Identifiers for the Subject Record • Identifiers for the Token Record *NB: Depending on deployment pattern specifications, the contained Identifiers may be 'opaque' or 'transparent' to the recipient. This may result in implementations that have been characterized as 'Pseudonymous Credential', 'Triple-Blind Credential Broker' or 'Monolithic'.*
User Account Record	• *a.k.a. The 'User Account' or 'User Profile' Record* • Identifiers that link the Credential to the User Account described in the User Account Record • Information about the User Account ○ Account Data ○ Account Metadata ○ User Preferences Data ○ Access Control data ○ May include 'ownership'; CRUD data
"Entity Record"	• An implied Record type that is not shown on the model. • Identifiers stored under the control of the Entity • Identifiers for locating the unique Identity Records and Token Records associated with this Entity

Record Type	Data Sets Stored & Examples
Logging and Audit Record	• Event information for activity in the systems and processes • Used for forensic investigation into data breaches • Used for operational management of services and systems

Functions in the General Model

The general model includes several Functions. As noted previously, a Function is a set of processes or activities that manipulate Records and Information stored in Records.

Note: ‘Credential’[4] and ‘Token’[5] are used according to the NIST SP800-63 usage.

Table 3: Functions And Their Record Types

Function	Purpose of Function	Record Type
Collect Subject Information	• Obtain attribute information from the Entity	Subject Record
Validate Subject Information	• Check the correctness of the collected information.	Subject Record
Verify Subject Information	• Check that the information pertains to the Entity that purports to be the Subject. • This is a core function of the “Identity Proofing Process”	Subject Record
Register Subject	• Create a Subject Record. • Generate identifiers for linking the Entity to the Subject Record. • Assert Identifiers to Entity to allow for later Subject Record matching. • Store Subject Attribute Data • Store Subject Metadata • Store Process Metadata	Subject Record
Assert Subject Information	• Assert Subject Information to authorized requester including relevant metadata (e.g. The Identity Proofing Level)	Subject Record
Update Subject Information	• Replace existing Subject Record Information with new version	Subject Record
Suspend Subject Information	• Prevent use of the Subject Record • May include an ‘Archive’ sub-function to allow for historical linkages to remain valid.	Subject Record
Delete Subject Record	• Delete the Subject Record • May include an ‘Archive’ sub-function to allow for historical linkages to remain valid.	Subject Record
Collect Token Information	• Obtain Token information and metadata ○ Tokens may be generated by a token generation system separate from the Token Manager	Token Record
Validate Token Information	• Check the correctness of the token information.	Token Record

[4] From NIST SP800-63-2: “An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.”

[5] From NIST SP800-63-2: “Something that the Claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the Claimant’s identity.”

Function	Purpose of Function	Record Type
Verify Token Information	• Check that the token pertains to the Entity that purports to bear the token. • *(This might be the same as Compare Token Authenticators)*	Token Record
Compare Token Authenticators[6]	• Compare the Token Authenticator presented by the Entity against the calculated or stored Token Authenticator derived or retrieved from the Token Record with the objective of verifying that the Entity possesses and controls the token. • May be known as Authentication, e-Authentication, Electronic Authentication, Authn • *(This might be the same as Verify Token Information)*	Token Record
Register Token	• Create a Token Record • Generate identifiers for linking the Entity to the Token Record • Assert Identifiers to Entity to allow for later Token Record Matching • Store Token Attribute Data • Store Token Metadata • Store Process Metadata	Token Record
Set Token State to Active	• Record the Token referred to in the Token Record as Active	Token Record
Assert Token Information	• Assert Token Information to authorized requester including relevant metadata	Token Record
Update Token Information	• Replace existing Token Record Information with new version	Token Record
Suspend Token Record	• Temporarily prevent use of the Token Record • May include an 'Archive' sub-function to allow for historical linkages to remain valid.	Token Record
Delete Token Record	• Delete the Token Record • May include an 'Archive' sub-function to allow for historical linkages to remain valid.	Token Record
Collect Credential Information	• Obtain Credential identifiers, information and metadata from (potentially) the Token Manager, Subject Record Manager and Online Service Provider •	Credential Record
Validate Credential Information	• Check the correctness of Credential information against the Records managed by the Manager Roles	Credential Record

[6] From NIST SP800-63-2: "The output value generated by a token. The ability to generate valid token authenticators on demand proves that the Claimant possesses and controls the token. Protocol messages sent to the Verifier are dependent upon the token authenticator, but they may or may not explicitly contain it."

Function	Purpose of Function	Record Type
Verify Credential Information	• Check the presence of Credential information against the Records managed by the Manager Roles • Might be the same as Index Verification	Credential Record
Register Credential	• Create a Credential Record • Retrieve asserted identifiers from (potentially) the Token Manager, Subject Record Manager and Online Service Provider • If applicable to the implementation, generate pseudonymous identifiers, Persistent Anonymous Identifiers, Meaningless But Unique Numbers, or Opaque Identifiers • Store Credential Attribute Data • Store Credential Metadata • Store Process Metadata	Credential Record
Set Credential State to Active	• Set the Credential Record state to Active	Credential Record
Assert Credential Information	• If applicable to the implementation, o Assert identifiers from the Credential Record OR o Generate and assert Session Identifiers derived from the identifiers from the Credential Record	Credential Record
Update Credential Information	• Replace existing Credential Record Information with new version	Credential Record
Suspend Credential Record	• Temporarily prevent use of the Credential Record • May include an ‘Archive’ sub-function to allow for historical linkages to remain valid.	Credential Record
Revoke Credential Record	• Cancel the Credential so that it cannot be used again • May include an ‘Archive’ sub-function to allow for historical linkages to remain valid.	Credential Record
Collect	• Obtain Credential identifiers, information and metadata from the Credential Manager • Obtain required information from the Subject Record Manager	User Account Record
Register User / Enroll for Services	• To create a service record or User Account Record for the purpose of providing services to the Entity	User Account Record
Update	• Replace existing User Account Record Information with new version	User Account Record
Suspend	• Temporarily prevent use of the User Account Record • May include an ‘Archive’ sub-function to allow for historical linkages to remain valid.	User Account Record
Delete	• Delete the User Account Record • May include an ‘Archive’ sub-function to allow for historical linkages to remain valid.	User Account Record
Create Log Record	• To record facts about events that occur within the system or identity solution	Logging and Audit Record

Function	Purpose of Function	Record Type
Investigate Incident	• To determine what events occurred, when they occurred and who was involved	Logging and Audit Record
Audit participants	• To determine conformance of operational service parameters	Logging and Audit Record
Accredit participants	NB: This paper does not enter into the area of Accreditation. Future versions might do so.	

Note: To distinguish the difference between a Function and a sub-function or an internal business process, consider processes that could be executed by a separate Entity as Functions. All processes that must be performed together within a single Entity should be considered to be internal business processes.

Roles in the General Model

The general model includes several Roles.

Organizations take on one or more Roles. Each Role is accountable for one or more Functions. For example, ACME Inc. could assume the Subject Record Manager Role, and is therefore accountable for the Functions associated with that Role.

The table shows the Roles and the Functions that are typically assigned. This model uses moderately granular Function definitions so that implementers can customize the Role-Function assignments to suit their designs.

Table 4: Roles and Typical Function Assignments

Role	Purpose and Typical Functions
Subject Record Manager (Identity Manager) (Attribute Manager)	Manages the full lifecycle of Subject Attribute and Identity information Functions: • Identify Entity (Collect attribute assertions) • Validate Identity attributes • Verify Identity attributes (Entity is the subject of the attributes asserted) • Register Identity information record • Assert Identity Attributes
Token Record Manager	Manages the full lifecycle of Token Records. Functions: • Collect Token Information • Validate Token Information • Verify Token Information • Register Token • Assert Token Information • Update Token Information • Suspend Token Record • Delete Token Record
Credential Record Manager	Manages the full lifecycle of Credential Records Functions: • Create Credential Record • Issue Credential (and manage throughout operational life) ~~• Authenticate Credential~~
Online Services Provider	Provides services to authorized entities. Functions: • Enroll Subjects/Entities for Services • Provide Services • Rely on Credential Manager, Token Manager and Subject Record Manager Roles for authentication information and subject information
Validator	Compares received information against a source (may be an authoritative or non-authoritative source) • Match information to source record

Andrew Hughes 10/7/13 10:52 AM
Formatted: Strikethrough, Highlight

Andrew Hughes 10/7/13 10:52 AM
Formatted: Strikethrough

Credential Broker	Intermediary that acts on behalf of other Organizations/Roles for several potential purposes: • Integration standardization or simplification • ‘Blinding’ the Roles from sources and targets • ‘Converter’ between different technologies or information formats
Entity	The Entity itself: • The Subject of the Records • A Person, Non-Person Entity or Organization • Provides attribute or identity information for Subject Records • Provides evidence to the degree required by the Identity Proofing Process at a given Assurance Level • Possesses Identifiers used to locate Subject Records and Token Records • Possesses Tokens used to authenticate the Entity’s Identity

“Deployment Patterns”

Overview

Definition

Implemented Deployment Patterns

FICAM-Approved Deployment

Description

Diagram

Special Characteristics

Covered Risks

Assignment of Liability

Flexibility

Privacy Enhancing Techniques

Role-Function Table

Includes variant mappings observed ‘in the wild’

Organization List

The list of Organization types that could receive Accreditation or Approval as envisioned in the deployment pattern.

Organization-Role Table

Includes variant mappings observed ‘in the wild’

Canadian Federal Government Deployment

Description

Diagram

Special Characteristics

Covered Risks

Assignment of Liability

Flexibility

Privacy Enhancing Techniques

Role-Function Table

Includes variant mappings observed ‘in the wild’

Organization List

The list of Organization types that could receive Accreditation or Approval as envisioned in the deployment pattern.

Organization-Role Table

Includes variant mappings observed ‘in the wild’

New Zealand Government Deployment

Description

Diagram

Special Characteristics

Covered Risks

Assignment of Liability

Flexibility

Privacy Enhancing Techniques

Role-Function Table

Includes variant mappings observed 'in the wild'

Organization List

The list of Organization types that could receive Accreditation or Approval as envisioned in the deployment pattern.

Organization-Role Table

Includes variant mappings observed 'in the wild'

UK Government Deployment

Description

Diagram

Special Characteristics

Covered Risks

Assignment of Liability

Flexibility

Privacy Enhancing Techniques

Role-Function Table

Includes variant mappings observed ‘in the wild’

Organization List

The list of Organization types that could receive Accreditation or Approval as envisioned in the deployment pattern.

Organization-Role Table

Includes variant mappings observed ‘in the wild’

SAFE BioPharma Deployment

Description

Diagram

Special Characteristics

Covered Risks

Assignment of Liability

Flexibility

Privacy Enhancing Techniques

Role-Function Table

Includes variant mappings observed ‘in the wild’

Organization List

The list of Organization types that could receive Accreditation or Approval as envisioned in the deployment pattern.

Organization-Role Table

Includes variant mappings observed ‘in the wild’

Modular FICAM Deployment

Description

Diagram

Special Characteristics

Covered Risks

Assignment of Liability

Flexibility

Privacy Enhancing Techniques

Role-Function Table

Includes variant mappings observed ‘in the wild’

Organization List

The list of Organization types that could receive Accreditation or Approval as envisioned in the deployment pattern.

Organization-Role Table

Includes variant mappings observed ‘in the wild’

InCommon Deployment

Description

Diagram

Special Characteristics

Covered Risks

Assignment of Liability

Flexibility

Privacy Enhancing Techniques

Role-Function Table

Includes variant mappings observed ‘in the wild’

Organization List

The list of Organization types that could receive Accreditation or Approval as envisioned in the deployment pattern.

Organization-Role Table

Includes variant mappings observed ‘in the wild’

WAYF Deployment

Description

Diagram

Special Characteristics

Covered Risks

Assignment of Liability

Flexibility

Privacy Enhancing Techniques

Role-Function Table

Includes variant mappings observed ‘in the wild’

Organization List

The list of Organization types that could receive Accreditation or Approval as envisioned in the deployment pattern.

Organization-Role Table

Includes variant mappings observed ‘in the wild’

Next Steps and Action Items

Appendix A: Certification, Accreditation and Trustmark Approval

Include AAS update – this will inform future edits. Also S3A update.

Discussion of selected ‘Trustmark’ Programs

Discussion of ‘Modularity’ implications for Accreditation

Appendix B: Kantara IAF Service Assessment Criteria

Mapping of Kantara IAF SAC to Services and Functions

Mapping of Kantara IAF SAC to Roles and Organizations