Functional Model Representation of the Identity Ecosystem

A structured representation of the functions within identity ecosystems

10/15/2015

Table of Contents

List of Tables

List of Figures

Revision History

Version 1.0	September 19, 2014	Adam Madlin

Introduction

Structure

The Identity Ecosystem Functional Model deliverable was developed by the IDESG Security Committee to provide context to discussions of identity ecosystems and a consistent model upon which to center descriptions of identity solutions. This is not a model of the IDESG as an organization but a representation of online identity interactions and the various components needed to execute those interactions.

The Security Committee first identified a preliminary set of Functional Elements (defined as the core set of functions that occur within the Identity Ecosystem) to serve as the foundation for functional model work and relevant evaluation methodologies. The efforts resulting in two complementary products that lay the ground work for future development of the Identity Ecosystem Functional Model:

- The Identity Ecosystem Functional Element Diagram, showing each of the functional elements, and
- The Identity Ecosystem Functional Element Description Matrix, providing a brief description of each of the core operations and elements.

In short, the functional elements are the "verbs" of identity-related activities online; they represent the possible activities that service providers[1] conduct in identity-related transactions. They do not, however encompass the whole of the identity ecosystem. In order to complete the model, three additional layers to the functional elements represent major components in the identity ecosystem:

- A governance layer involving activities such as policy and rule development, certification, accreditation, and assessment and
- An interoperability layer involving activities such standards and specification development and exchange technologies, and
- An administration and operations layer involving activities such as performing redress and internal auditing within the functional elements.

Purpose and Use

The purpose of the functional model deliverable is to identify and describe common operations, functions, roles, and activities applicable to the broadest set of Identity Ecosystem use cases possible. The model's primary purpose is to provide a consistent model upon which to center descriptions of identity solutions. The functional model deliverable can facilitate and support several other work streams of the IDESG, including:

- Support the development of IDESG requirements and best practices,
- Highlight common technical and policy considerations for interoperability,
- Set conditions for mutual recognition of existing trust frameworks/federations,
- Facilitate consistency for service provider descriptions of the activities they conduct in online interactions,

[1] The term service provider covers the roles identified in the Functional Model except for the User role.

- A broad way to organize a certification and accreditation program for the IDESG.

As the functional model deliverable is primarily a descriptive tool, the model provides only high-level descriptions to ensure maximum coverage without being dependent upon existing or pre-determined ecosystem roles. The goal is to establish common operations, functions, and roles that are applicable across environments, technologies, and interaction types. The operations and actions could be executed at different times, in different orders, and by different actors, depending on the use case, and each is intended to be considered independent of the others.

The primary purpose of this document is to provide a consistent model for describing identity ecosystem services, however, the security committee intends for it to be extensible and flexible so that it can be used to facilitate other IDESG work as well.

Maintenance

The security committee will maintain and update the document but other IDESG committees may request changes as necessary. For more information about this document and the maintenance of it see the IDESG wiki under Functional Model.

Functional Model

The functional model consists of four layers: functional elements, administration and operations, interoperability, and governance and accountability. This section details each of these layers.

Functional Model Diagram

The functional model diagram provides the activities that occur in the governance, interoperability, and administration and operations layers, the core operations in the functional elements layer and the roles in which entities engage at each of the four layers. The order of appearance of the layers does not indicate a priority or preference.

Figure 1. The Identity Ecosystem Functional Model

Functional Elements Layer

The functional elements layer consists of functional elements—the basic operations that may occur in online identity-related interactions—grouped into core operations. Not all elements will be invoked in every identity interaction, and some may be invoked multiple times. While logically some functions are likely to occur before or after others, there is no explicit order specified in the model.

Figure 2. Functional Elements Layer

Functional Elements Diagram

To improve readability, the functional elements layer is presented in a single diagram including all functional elements and core operations.

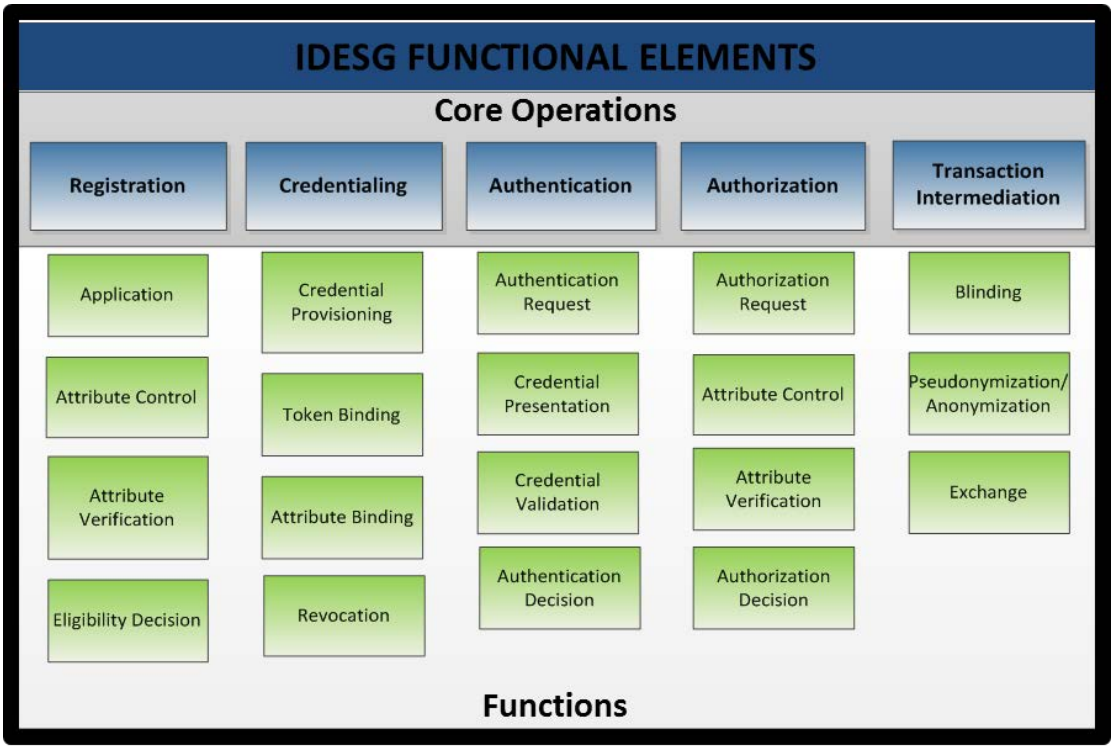

Figure 3. Identity Ecosystem Functional Elements

Functional Elements Description Matrix

The functional elements description matrix provides brief descriptions of each core operation and functional element.

Core Operation	Function	Description
Registration		Process that establishes a digital identity for the purpose of issuing or associating a credential.
	Application	Process by which an entity or agent requests initiation of registration.
	Attribute Control	Process of managing and releasing attributes for the purposes of registration or authorization.
	Attribute Verification	Process of confirming or denying that claimed identity attributes are correct and meet the pre-determined requirements for accuracy, assurance, etc.
	Eligibility Decision	Decision that an entity does or does not meet the pre-determined eligibility requirements for a digital identity or credential.
Credentialing		Process to bind an established digital identity with a credential.
	Credential Provisioning	Process by which ownership of a credential is conferred, confirmed, or associated with a digital identity.
	Token Binding	Process of binding a physical or electronic token to a credential.
	Attribute Binding	Process of binding attributes to a credential.
	Revocation	Process by which an issuing authority renders a digital identity, issued credential, token, or verified attribute invalid for authentication or authorization.
Authentication		Process of determining the validity of one or more credentials used to claim a digital identity.
	Authentication Request	Process by which authentication is initiated by an entity.
	Credential Presentation	Process by which an entity submits a credential for the purposes of authentication.
	Credential Validation	Process of establishing the validity of the presented credential.
	Authentication Decision	Decision to accept or not accept the results of the credential validation process.
Authorization		Process of granting or denying specific requests for access to resources.
	Authorization Request	Process by which authorization is initiated by an entity.
	Attribute Control	Process of managing and releasing attributes for the purposes of registration or authorization.

Core Operation	Function	Description
	Attribute Verification	Process of confirming or denying that claimed attributes are correct and meet the pre-determined requirements for authorization; typically, these attributes for authorization have not been bound to the credential or previously available to the organization making the authorization decision.
	Authorization Decision	Decision to grant and deny access to a resource based on the results of the authorization processes and policies.
Transaction Intermediation		Processes and procedures that limit linkages between transactions and facilitate credential portability.
	Blinding	Process by which service providers involved in a transaction are prevented from observing each other (i.e., a relying party does not know which credential service provider an entity is utilizing in a transaction or vice versa). Based upon the transaction type and the number of service providers involved, blinding may be done to prevent a single, multiple, or all service providers from viewing the other participating services.
	Pseudonymization/ Anonymization	Process by which an intermediary prevents service providers from linking a digital identity with a particular person or entity.
	Exchange	Process by which one protocol is translated to another for consumption by different entities involved in a transaction.

Table 1. Functional Elements Description Matrix

Functional Element Layer Roles

Table 2 provides descriptions of the roles in the functional elements layer. These are intended to provide ecosystem participants with a common understanding of the functions typically executed by the identified roles. Note that an ecosystem participant may serve more than one role and serving a role does not require the participant to execute all of the functions in that role. Additionally, this list is not intended to restrict organizations from executing any of the ecosystem functions.

Role	Description	Functions Executed
User	Person or non-person entity attempting to establish a digital identity and/or use a credential to access a protected resource.	*Application, Attribute Control, Credential Presentation, Authorization Request*
Credential Service Provider (CSP)	Entity that manages the credentialing and authentication core operations.	*Credential Provisioning, Token Binding, Attribute Binding, Revocation, Credential Presentation, Credential Validation, Authentication Decision*
Authentication Service Provider	Entity that manages authentication core operations.	*Credential Validation, Authentication Decision*

Role	Description	Functions Executed
Registration Authority (RA)	Entity that manages the registration core operation.	*Attribute Control, Attribute Verification, Eligibility Decision, Updates (Periodic & Event Based)*
Identity Provider (IDP)	Entity that manages the registration, credentialing, and authentication core operation.	*Attribute Control, Attribute Verification, Eligibility Decision, Updates (Periodic & Event Based), Credential Provisioning, Credential Provisioning, Token Binding, Attribute Binding, Revocation, Credential Presentation, Credential Validation, Authentication Decision*
Attribute Provider (AP)	Entity that executes the attribute verification and attribute control functions in support of the core operations.	*Attribute Verification, Attribute Control, Updates, Revocation*
Relying Party (RP)	Entity that relies upon other entities to execute the core operations and functions in order to authorize access to protected resources.	*Eligibility Decision, Authorization Decision,* *Attribute Binding*[2]
Intermediary[3]	Entity that executes the transaction intermediary core operation.[4]	*Blinding, Pseudonymization/Anonymization, Exchange*

Table 2. Functional Element Layer Roles

[2] The inclusion of this function serves as an acknowledgement that some RPs conduct attribute binding to user accounts for managing user preferences, conducting identity resolution, or other transactional purposes.

[3] This role may be filled by any service provider (e.g., organization, device, application) that executes the identified core operation and functions. As with all the core operations, this is a set of operations that do or can exist in identity systems and, in turn, could have associated standards and requirements that apply to them.

Administration and Operations Layer

The layer at which entities execute activities intended to administer and support the IDESG core operations and functions. All members of the ecosystem that execute functional layer roles will also execute the activities in the administration and operations layer.

Figure 4. Administration and Operations Layer

Table 3 provides descriptions of the activities in the administration and operations layer

Activity	Description
Redress	Process by which entities and organizations reconcile errors that occur during the operations and processes of an identity system. All ecosystem service providers must execute redress activities.
Recovery	Process and procedures by which an organization ensures availability and continuity of credentials, attributes, and other identity services following a security or privacy event (e.g., data breach, disruption of services, etc.) All ecosystem participants are responsible for executing recovery activities.
Enterprise Governance	Process by which entities develop and implement necessary policies and rules to support proper execution of core operations and functions (e.g., legal agreements/policies, data protection policies, security policies, privacy policies, etc.)
Internal Audit	Process of reviewing and collecting evidence of an entity's conformance with enterprise rules, policies, and requirements.
Service Optimization	Process by which organizations take internal and external inputs (e.g., standards, customer surveys, or external governance/regulation) and integrate them in order to improve execution of the service.
Updates (Periodic & Event Based)	Process by which an entity updates accounts, attributes, credentials, and other identity information to determine eligibility for an entitlement; may be periodic in nature or event based (e.g., marriage, end of subscription, etc.)

Table 3. Administration and Operations Layer

Interoperability Layer

The interoperability layer is that at which entities in the ecosystem establish and maintain the ability to communicate and exchange identity data

Figure 5. Interoperability Layer

Table 44 provides descriptions of the activities and descriptions in the interoperability layer.

Category	Description
Activity	
Standards Development	Process of creating standards for identity technologies and procedures to be used within communities or across the ecosystem.
Specification Development	Process of creating the specifications and profiles that define how participants in a community assert and exchange identity data.
Exchange	The process of facilitating technical (including semantic) interoperability to support credential portability between participants within a specific community or across the ecosystem.
Role	
Standards Development Body	Entity responsible for creating identity standards for a specific community or the ecosystem.
Specification Development Body	Entity responsible for creating identity specifications.
Interoperability Providers	Entities responsible for facilitating technical interoperability between participants across entities and communities of the ecosystem, such as federation operators and exchanges (e.g., attribute, credential).

Table 4. Interoperability Layer Activities and Roles

Governance & Accountability Layer

The layer at which entities create, monitor, and enforce rules, guidelines, and requirements for executing the IDESG functional elements across communities or actors. Unlike the administration and operations layer, the governance and accountability layer is specifically intended to address cross entity efforts rather than enterprise or internal governance.

Figure 6. Governance Layer

Table 55 provides descriptions of the activities and descriptions in the interoperability layer.

Category	Description
Activity	
Policy / Rule/ Requirements Development	Process of creating a trust framework including identifying or adopting rules, requirements, and policy for governing the use of identities and identity technology within a specific community.
Accreditation	Processes for the evaluation, approval and formal recognition that an entity is capable of carrying out certification or assessment activities for a trust framework.
Certification	Processes of assessing, validating, and determining that a product or service provider meets the defined requirements of a trust framework.
Assessment/Audit	Process of reviewing and collecting evidence of an entity's conformance with the rules, policies, and requirements for a trust framework or community.
Roles	
Community of Interest	A group of entities that establish a trust framework.
Accreditation Body	Entity responsible for conducting accreditation activities for a trust framework.
Certification Body	Entity responsible for conducting certification activities for a trust framework.
Assessor/Auditor	Entity that conducts assessments of participants in a trust framework or community; these can support accreditation or certification.

Table 5. Governance Layer Activities and Roles