An approach to separation of credential provision functions from identity attribute functions in the KI IAF and SAC

Andrew Hughes, in collaboration with Ken Dagg, David Wasley and Colin Soutar:
Kantara Initiative Identity Assurance Working Group

October 2012

Introduction

This document is the result of extensive discussions between Andrew Hughes, Ken Dagg, David Wasley and Colin Soutar of the Kantara Initiative Identity Assurance Working Group. It is part of a larger migration towards a more flexible assurance and conformance model that can accommodate multiple trust framework arrangements.

The goal of the Identity Assurance Framework, and related Service Assessment Criteria, is that a Relying Party, which is consuming assertions based on a credential to make operational decisions, can be confident to the specified level of assurance that the assertion represents the particular entity using the credential, as recorded by a Credential Service Provider. The current Identity Assurance Framework and related Service Assessment Criteria are based on a model that requires identification of the credential requester prior to credential issuance. This model constrains flexibility and scalability of implementations because every provider of credentials must take on both the functions, roles and obligations of a Credential Service Provider (CSP) and an Identity Service Provider (IDSP). We contend that this dual role is not essential and that other models may have important advantages, such as an ability to abide by privacy constraints.

This document describes an analysis of the current model and sets out the refinements and model changes required to make the identification of persons and the issuing of credentials separable. The binding of a credential to an identity then can be accomplished in various ways depending on requirements of Relying Parties, or the trust framework arrangement.

The analysis approach used was to separate the Actors, Roles, Functions and their Relationships into discrete elements. These elements were then organized into a general model for describing the current thinking on how Credential Service Providers could be made separate from Identity Service Providers. The general model can represent the currently known approaches contemplated to achieve this separation.

Once the more flexible general model is sufficiently developed, with several approaches modeled with it, specific changes needed for the IAF and SAC can be outlined.

It will be clear that this flexible model supports a transactional level of assurance that is the composite of the assurance of the credential management process and the assurance of the identity assertion, regardless of when these steps occur.

Note that the separation of Identity Service Provider and Credential Management functions will enable flexible systems to be deployed, including high assurance systems where the identity proofing is required to underpin the issued credential, such as is contemplated in PIV-I.

A note on terminology

The Kantara Initiative Glossary is the baseline for terms used in this document. Novel terms or new usages contained in this document are described in the Terminology section.

Contents

Introduction 1

General Model Elements 4

Approaches to Credential and Identity Lifecycle Management Arrangements 4

Actors, Roles and Functions 5

Functions 6

Roles 7

Actors and Entities 7

Entities 7

Record linkages and bindings 8

The General Model 8

The Current model – NIST SP800-63 Based Model 9

Current model functional assignments 9

The Proposed model – The “Decoupled Binding” Model 11

Proposed model functional assignments 12

The “Pseudonymous Approach” 13

Modifications recommended for IAF and SAC 13

Terminology 14

Table of Figures

Figure 1 - The General Model Elements 9

Figure 2 - Current Model 10

Figure 3 - Proposed Model 12

General Model Elements

This section describes the elements that make up the general model, using a functional analysis approach.

The major Functions, Roles and Relationships are first identified to make up the general model.

Describing the range of implementation approaches then becomes a simple exercise in assigning Roles to Actors.

Approaches to Credential and Identity Lifecycle Management Arrangements

In this document, we explicitly describe the following approaches:

Approach Name	Key Characteristics
NIST SP800-63	Credential Manager [1]and Identity Manager Roles assigned to a Credential Service Provider Actor, and Functions intermixed. This is the Current Model, based on NIST SP800-63.
Decoupled Binding Approach	Credential Manager and Identity Manager Roles assigned to different Actors. Credential-Identity Link Manager Role assigned to Relying Party Actor. This is the Proposed Model, sometimes known as the "Pseudonymous Credential Model"
Credential Broker Approach *(Described in the next paper in the series[2])*	Credential Manager and Identity Manager Roles assigned to different Actors. Credential-Identity Link Manager Role assigned to separate Credential Broker Service Provider Actor.
Credential Broker (Internal) Approach *(Described in the next paper in the series)*	Credential Manager and Identity Manager Roles assigned to different Actors. Credential-Identity Link Manager Role assigned to Credential Broker Service Provider Actor which is within the Identity Manager organization.

[1] See the Terminology section for term definitions

[2] For clarity, this paper only discusses the current NIST SP800-63 based model and one alternative model for the Decoupled Binding Approach. A future paper will elaborate on the Credential Broker Approach and model.

Actors, Roles and Functions

In this paper, we have defined three elements that are used to describe the interactions and responsibilities in the models.

Model Element	Description
Actor	An Actor is an abstract term that represents an Entity in the models. Actors assigned to a Role perform and are accountable for the Functions associated with that Role. An Actor can be assigned to zero, one or many Roles.
Role	A Role is an abstract term that represents a set of Functions in the models. A Role is assigned to the Actor responsible for performing the related Functions. Roles can be assigned or associated with zero, one or many Actors or Functions.
Function	A Function is an abstract term that represents activities or processes performed by Actors in the models. Functions can be composed of other Functions. Similar Functions can be associated with zero, one or many Roles.

Functions

The general model includes several Functions.

Function	Purpose
Identify Individual	The use of processes by the Registrar to obtain identity facts/attributes from the Individual for verification to a level of assurance.
Validate Identity	To provide assurance of the correctness of identity facts/attributes to a registering or enrolling entity at the requested LOA.
Verify Identity	To provide assurance at the requested LOA that the identity facts/attributes presented by an Entity actually refer to that Entity.
Register Entity	To create an identity record for an entity containing a unique Entity identifier, identity facts/attributes (or pointers to other service providers with them), and other facts/attributes (or pointers to other service providers with them). The specific facts stored are determined by the interaction model specifications.
Provide Identity Attributes	To provide identity attributes at a level of assurance to a relying party
Activate/Create Credential	To create a valid and active credential which contains a unique identifier for the credential Subject.
Issue Credential	To provide the Entity with a valid and active credential and record the unique Subject identifier plus facts about the issuance processes
Authenticate Credential	To ensure to a level of assurance that the entity that is presenting the credential at a later time is the same entity to which it was issued.
Enroll for Services	To create a service record or subject record for an Entity.
Provide Services	To locate the service or subject record and provide the Entity with entitled services as recorded.
Assert Identity	Provide identity attributes/facts and evidence when requested for enrollment or registration.

Roles

The general model includes several Roles.

Role	Purpose and Functions
Credential Manager	Manages the full lifecycle of electronic credentials Functions: - Activate/Create Credential - Issue Credential (and manage throughout operational life) - Authenticate Credential
Identity Manager (Attribute Manager)	Manages the full lifecycle of electronic 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 - Provide Identity Attributes
Online Services Provider	Provides services to authorized entities. Functions: - Enroll for Services - Provide Services
Individual Role	Assert Identity attributes and provide evidence Receive Service

Actors and Entities

The general model includes several Actors. An Actor is the abstract element that forms part of the model. Actors are named according to their associated "Real World" Entity.

The Entity is the name of a real individual, organization or device. In this paper, Entities are named according to their type. In more detailed models of actual implementations, Entities would be specifically named.

Each Actor in the model should have one Entity associated with it. To describe the case where an Entity performs multiple Roles, associate the Entity with each of the Actors associated with the roles.

Entities

Entity	Description
Individual	A "Real" person; generally the Subject bound to a credential
Credential Service Provider	A "Real" provider of credential services
Identity Service Provider	A "Real" provider of identity services. An Identity Service Provider is a specialized Attribute Service Provider.

Attribute Service Provider	A “Real” provider of attribute services
Relying Party	“Real” provider of online services. Relies on assertions from Credential Service Providers, Identity Service Providers, Attribute Service Providers, Credential Brokers and Individuals.

Record linkages and bindings

The issuance of a credential to a person and identity proofing processes have often been described as ‘Binding’ the real person to the credential. This refers to the Credential Manager Role or Identity Manager Role creating a record that contains a unique reference to the individual and credential for the former, and the individual and identity record for the latter.

Increasing levels of assurance are said to have ‘stronger’ bindings due to the increased process rigour and increased security, evidence and verification stringency required.

An objective of electronic credential systems used to control access to online services is to ensure that the entity-credential-identity record bindings are sufficiently strong to permit the Relying Party to manage risks related to mis-identification or fraudulent use of credentials. It is assumed that the bindings are transitive: A bound to B and B bound to C means that A is also bound to C.

The bindings envisioned include:

Role	Relationship recorded
Identity Manager	Entity to Identity Information Record
Credential Manager	Entity to Credential Record
Credential-Identity Link Manager	Credential-Identity Linking Record

The General Model

The General Model contains all of the Roles, Functions and Actors. A high level diagram in this section shows the fundamental relationships between these elements.

Each specific model is based on the framework of the General Model. The difference between each specific model is in the assignment of Actors to Roles – in other words, the details of which Entities are accountable for performing which group of Functions.

This general model can be used to describe the current situation where a Credential Service Provider takes on the Credential Manager Role functions plus the Identity Manager Role functions. Or, it could describe a situation where the Credential Manager and Identity Manager Role functions are performed by separate Actors.

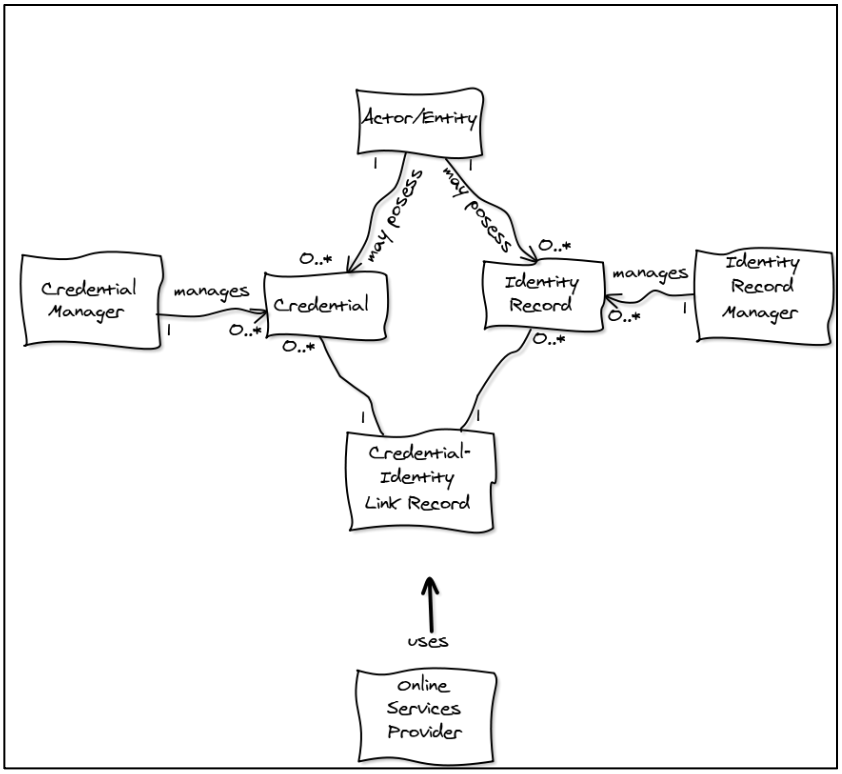

Figure 1 - The General Model Elements

The Current model – NIST SP800-63 Based Model

Current model functional assignments

In the current model, based on NIST SP800-63, there are three primary actors: the Credential Service Provider, the Actor/Entity and the Relying Party.

The Functions are allocated in this way:

Actor	Role (s)	Functions
Credential Service Provider	Credential Manager Identity Manager	Identify Entity Validate Identity Verify Identity Register Entity Activate/Create Credential Issue Credential Authenticate Credential
Relying Party	Online Services Provider	Enroll for Services Provide Services
Entity	Entity	Assert Identity Attributes and provide evidence Receive service

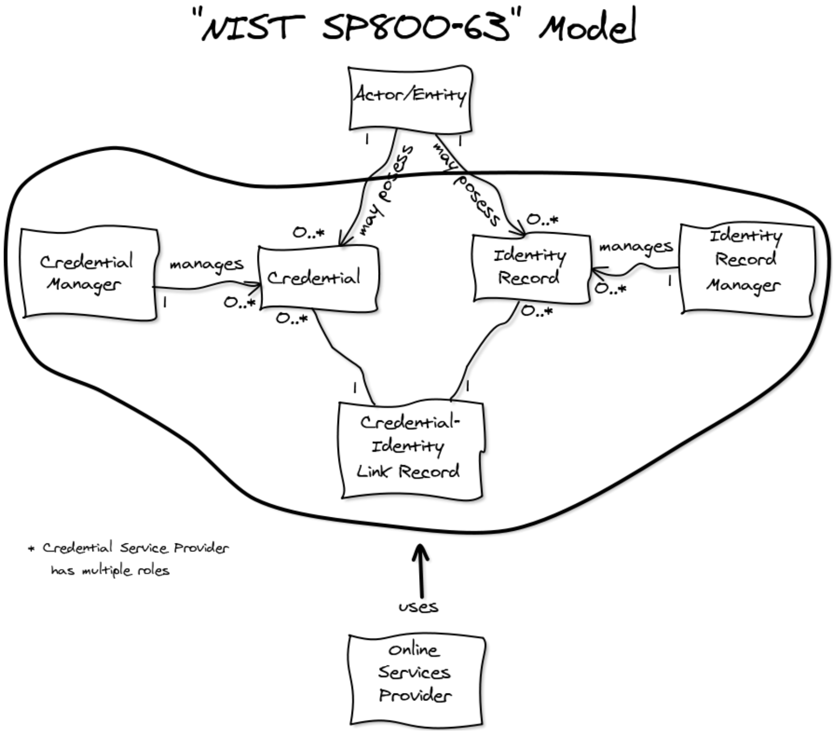

Figure 2 - Current Model

In the figure above, the Credential Service Provider has the Credential Manager Role and the Identity Manager Role.

The IAF and SAC have specifications and conformance clauses which require the Credential Service Provider to perform both the identity functions (Identify Entity, Verify Identity, Validate Identity, Register Entity) and credential functions (Activate/Create Credential, Issue Credential, and Authenticate Credential). This requirement prevents separation of the identity and credential functions into separate providers.

The Proposed model – The “Decoupled Binding” Model

If we think of the purpose of an on-line digital credential as fundamentally a way to bind a unique identifier to a particular physical entity then the requirements for reliability and trustworthiness of that credential are only about how that and only that physical entity can prove possession of that credential. Once we are confident in that binding, then one or more on-line service providers can begin associating various aspects of real world identity of the credential holder with the unique identifier in that credential.

A Credential Service Provider can focus on the issuance and life cycle management of various kinds of on-line credentials. Standards describing credentials, including multi-factor credentials, will define credential Level of Assurance only in terms of the binding of a unique identifier to a particular physical person.

This model makes no assumptions about what identity information might be important or useful to Relying Parties. In fact, On-line Service Providers could ignore all such information as part of registering a customer for their service offerings, relying only on the strength of the binding of the credential identifier to a particular physical entity. Different IDSPs could offer reliable assertions to other Relying Parties depending on what information the RP needs to know. For example, an employer could serve as an IDSP for RPs that provide services to its employees. A university could serve as an IDSP for RPs that provide services to its faculty and/or students.

This model makes no assumption about how many credentials a particular individual might have. Some might prefer the convenience of a single credential for multiple activities (for example, stored in a convenient form factor, such as a cell phone); others might prefer, for whatever reason (i.e., perception of improved privacy), to use different credentials for different aspects of their lives.

Flexibility of role assignments, the ability to create specialized Attribute Managers and scalability are the major benefits of the alternative model. The paper “Rethinking On-line Credentials and Identity” describes these benefits in greater depth.

Proposed model functional assignments

In the proposed model, a new primary actor is envisioned: the Identity Manager (or Attribute Manager).

The Functions are allocated in the following way. Note that the functions listed are strictly from the General Model catalog of functions; there are additional functions for the Roles that are not in this document.

Role	Functions
Credential Manager	Activate/Create Credential Issue Credential Authenticate Credential
Identity Manager (Attribute Manager)	Identify Entity Verify Identity Attributes Validate Identity Attributes Register Identity Information Record Provide Identity proof and facts
Online Services Provider	Enroll for Services Provide Services
Individual/Entity	Assert Identity Attributes and provide evidence

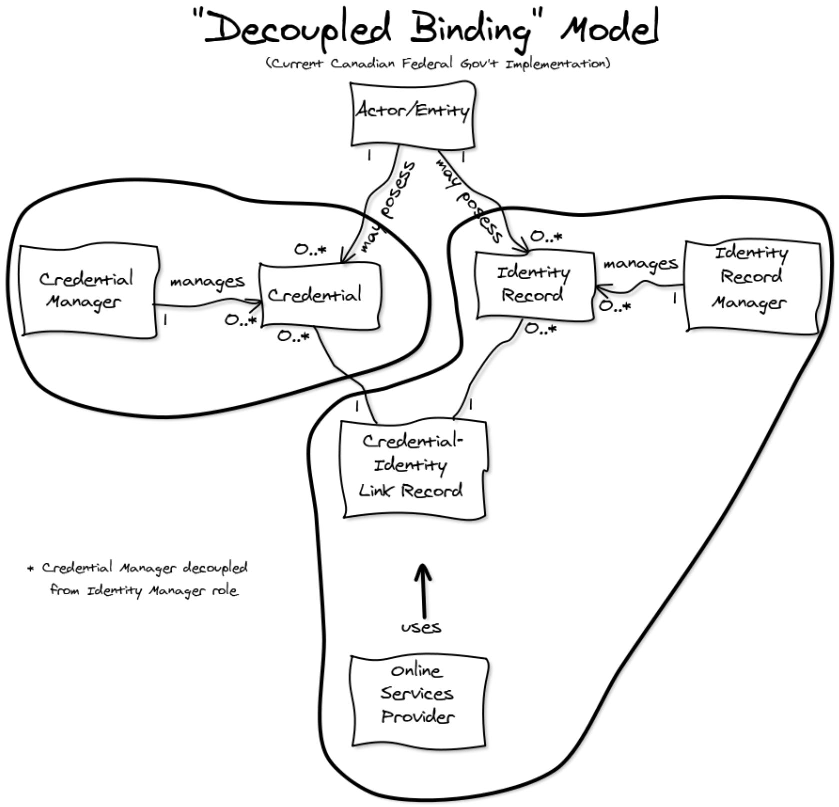

Figure 3 - Proposed Model

In the figure above, the Credential Service Provider has the Credential Manager Role. The Online Services Provider has the Identity Manager Role.

The “Pseudonymous Approach”

Within the IAWG, the term “Pseudonymous Approach” has been used to describe some of the characteristics of the proposed model. Specifically, it is the Credential which is considered to be pseudonymous because personally identifying information would no longer be transmitted along with the credential, and the Credential Service Provider would have no obligations to identify the ‘real’ person receiving the credential. The CSP must be able to determine if the current holder of the credential is the same entity that originally received the credential. This can be accomplished by means that do not involve personally identifying information, for example, by using shared secrets.

Fully realized, this Decoupled Binding or Pseudonymous Crednetial approach assumes that:

- identity attribute records are stored by the Identity/Attribute Manager Role (noting that this Role might actually be performed by a Relying Party or an Authoritative Source);
- credentials do not contain personally identifying information;
- Relying Parties can make access decisions based solely on credential presentation and do not necessarily require personally identifying information;
- any number of Identity/Attribute Managers, Credential Managers and Online Service Provider Actors may exist;
- a credential is linkable within connected inter-federations which use compatible trust frameworks; and,
- the order of functions is flexible (e.g. the identity validation and verification process could occur prior to or after the credential issuing process).It should be noted that the pseudonymous approach does not preclude other process arrangements.

Modifications recommended for IAF and SAC

In order to move to the proposed model, several changes are required in the IAF and SAC. Specifically, any clauses that require a CSP to identify the individual and embed this information within the credential would change.

In order to avoid issues existing trust framework providers, or to previously certified organizations, these changes should be made in a way that maintains equivalence to the original clause. Over time, it may become possible to separate the clause components into separate clauses.

Further work is needed to identify the specific clauses needing changes, and to suggest the actual changes. Changes may also be required to the IAF Glossary.

Terminology

This section describes the novel terms used within this document.

Term	Meaning
Entity	The Entity is the name of a real individual, organization or device. In this paper, Entities are named according to their type. In more detailed models of actual implementations, Entities would be specifically named.
Individual (Entity)	A "Real" person
Credential Service Provider (Entity)	"Real" provider of credential services
Identity Service Provider (Entity)	"Real" provider of identity services
Attribute Service Provider (Entity)	"Real" provider of attribute services
Relying Party (Entity)	"Real" provider of online services. Relies on assertions from Credential Service Providers, Identity Service Providers, Attribute Service Providers, Credential Brokers and Individuals.
Actor	An abstract term that represents an Entity in the models. Actors assigned to a Role perform and are accountable for the Functions associated with that Role An Actor can be assigned to zero, one or many Roles.
Role	An abstract term that represents a set of Functions in the models. A Role is assigned to the Actor responsible for performing the related Functions. Roles can be assigned or associated with zero, one or many Actors or Functions.

Function	An abstract term that represents activities or processes performed by Actors in the models. Functions can be composed of other Functions. Functions can be associated with zero, one or many Roles.
Record	An abstract term that represents a set of stored values. In this model, Records are used to hold identifiers, serial numbers and their relationships. In this modeling approach, Records are managed by 'Manager' Roles.
Credential Record	A record that contains details required for Credential lifecycle management.
Identity Information Record	A record that contains identity attribute information and details required for Identity lifecycle management.
Service Record	A record that describes the services allocated to Entities. Could be considered as a form of service access control/authorization record.
Credential-Identity Link Record	A record containing linkages between credentials and identity records.
Credential Manager Role	An abstract term associated with credential lifecycle management Functions. Manager of credential lifecycle management records (Credential Records)
Identity Manager Role	An abstract term associated with identity attribute lifecycle management Functions. Manager of Identity Information Records.
Online Service Provider Role	Provides online services. If assigned to the Relying Party Entity, relies on assertions from Credential Service Providers, Identity Service Providers, Attribute Service Providers and Individuals.
Identity Validation	Confirmation that the identity facts presented by an Actor are correct.

Identity Verification	Confirmation that identity facts presented by an Actor actually refer to that Actor. Answers the question: “Do these facts refer to you?”