Kantara IAWG
Sub-group report

Approaches to separation of Identity and Credential Management in IAF and SAC

October 2012

Andrew Hughes, Ken Dagg, David Wasley, Colin Soutar

The Situation

- IAWG Roadmap task to identify work required to implement the 'Pseudonymous approach' to credential management by end-Q3 2012
- Recent work completed to restructure IAF-SAC into assessment of 'component' services: identity and credential
  - Did not change the requirement that CSP handles both the credential manager role and identity manager role

SAC 'Component' version v Decoupled Binding approaches

- The SAC Component Services version describes how a service provider may be assessed for either Identity or Credential service provision.
- Note: FICAM/NIST SP800-63 require that the credential service provider is the same organization as the identity provider.
- If that requirement is removed, then alternatives exist for organizations to take on one or many roles. i.e. the CSP and IdP could be different organizations

Our Summer Discussions

- Discussion over the summer to decide on what the sub-group was attempting
  - Modify SAC? Define Identity-Credential Separation?
- Was clear that each person conceived different problem spaces
  - Determined that there was no known model showing the actors, functions and roles underlying IAF-SAC
- Decided that correct name is closer to "Decoupled Binding" approach
- In September, clear enough scope to write current document

The Result

- Decided that the sub-team would define the model of the current and target arrangements, THEN look at what needs doing with SAC
- Defined a general model showing Functions, Roles, Actors and some interactions
- Defined the terms needed for the model
- Assigned Roles to Functions & Actors to Roles for:
  - Current NIST SP800-63 based model
  - Proposed 'Decoupled Binding' model

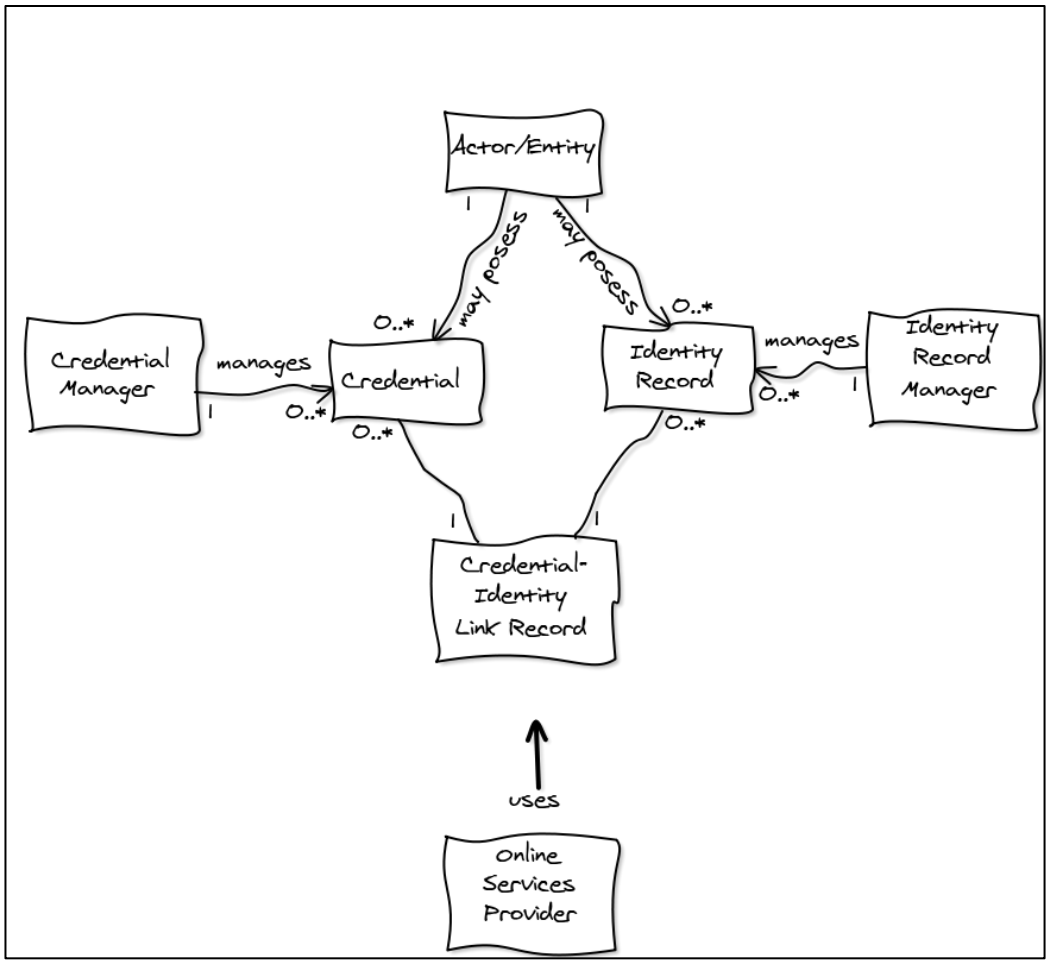
What's this model thing?

- Model shows the abstract working parts of the 'system' and how they interact
- The General Model based on a loose functional decomposition of the Identity Manager and Credential Manager role concepts
- Provides a simplified, common basis for shared understanding
- Should make it easier to debate what's where

General Model Elements

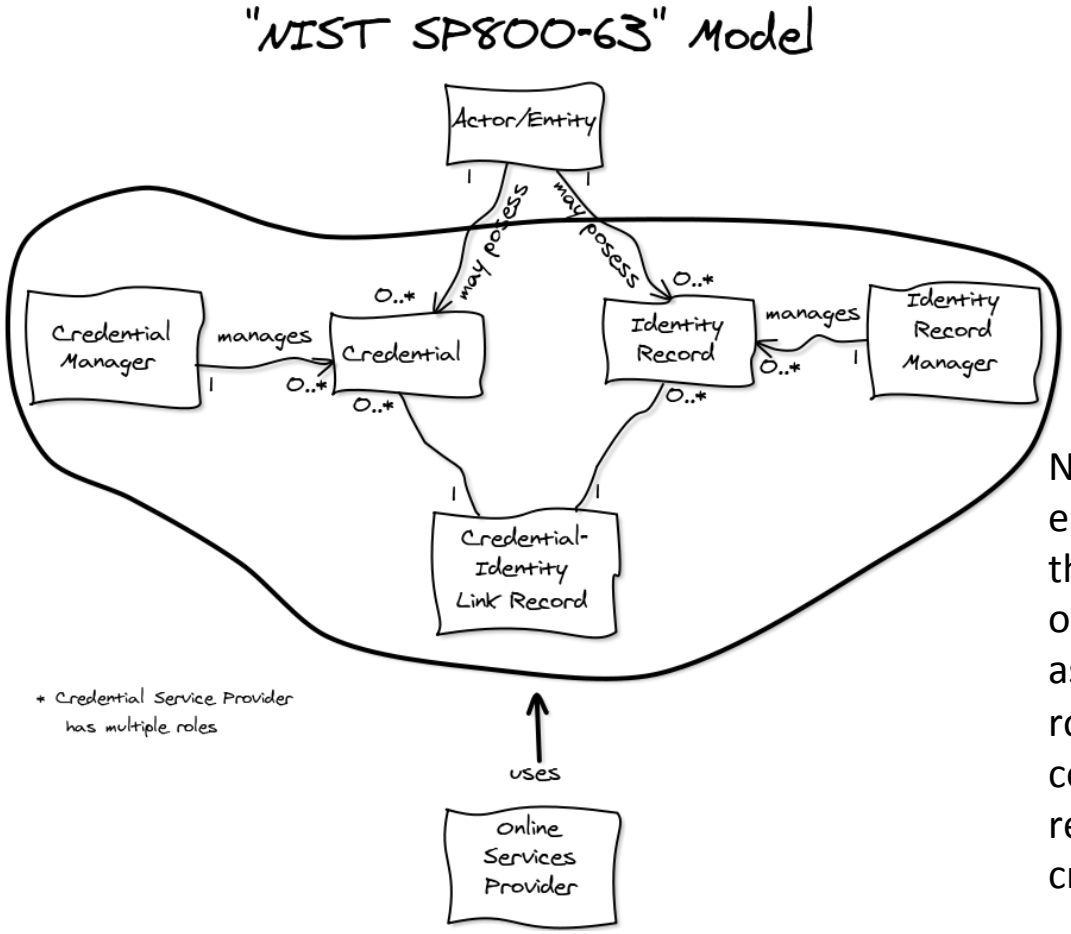
- Function
  - A process or activity carried out by an Actor
  - Assigned Actor is accountable for the Function
- Role
  - Logical, abstract way to group related Functions
  - Role assignments to Actors are the differences between the Approaches
- Actor
  - Abstract entity that takes action or is acted upon

The General Model



Note: the Model diagrams show the relationships between the different types of records and the manager of those records.
It does not show time or sequence.
It does not show Role to 'real' Organization assignment.

NIST SP800-63 Approach

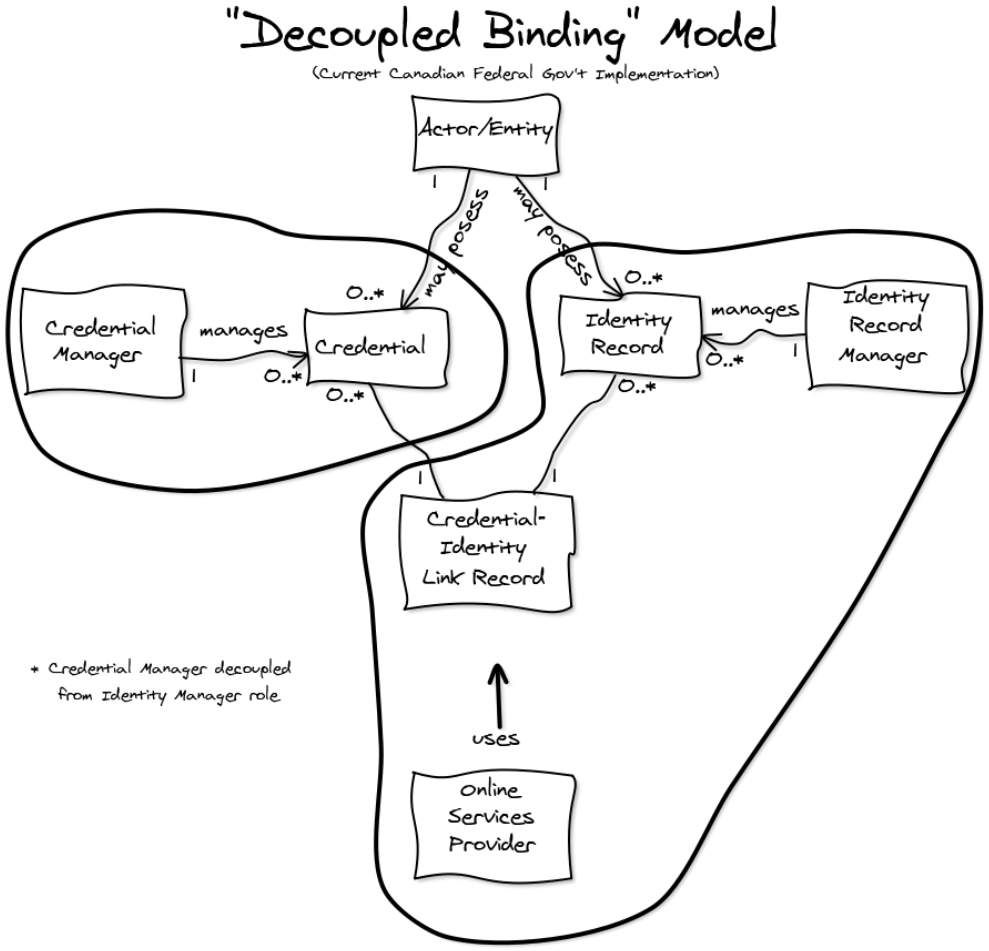


Note: the circled elements indicate that a single 'real' organization is assigned those roles and has control over the records or credentials.

NIST SP800-63 Approach

- The roles of Credential Manager and Identity Manager are performed by the Credential Service Provider (in the circle)
- Function-Role definitions are intertwined, hard to detangle without rewrite

“Decoupled Binding” Approach



Note: the circled elements indicate that a single ‘real’ organization is assigned those roles and has control over the records or credentials.

A Decoupled Binding Approach

- Credential Manager Role performed by Credential Service Provider
- Identity Manager Role and Linker done by Online Services Provider (a.k.a. Relying Party)
- Key is that Relying Party keeps identifying information AND Service information; does not know exactly who got the credential just that it's the same person

Other Approaches

- Credential Broker Role
  - New role to manage the Credential-Identity Link Records
  - Can be ‘triple-blind’ to hide Manager identifiers and orchestrate authentication sequences
  - Can be external party