Manage Digital Identities - Administration and Delegation

Brief Description

This covers the process by which a person receives an initial digital identity or updates an existing digital identity when verification of identity cannot be handled using self-service tools. This can be due to a need for higher level of verification of identity or an inability by an individual to use the self-service tools.

Generic Functional Requirements

- Automated creation of initial digital identity based upon on-boarding data from source systems
- Automated expiration of a digital identity based upon data from source systems
- Ability to recognize and consolidate identities for an individual if the individual exists in more than one source system
- Allows for the delegation of tasks based on customer identity (such as "the students in my department")
- Allows for the delegation of tasks based on user's level of access (ie super user, assist students only, work only from a specific set of machines)
- Ability to issue a single use token for resetting of passphrase
- Ability to view/search relevant data in the system
- Ability to update data which is not based on source system data
- Ability to expire or delete a digital identity
- Ability to track authorization levels based upon level of verification of identity
- Ability to allow a 3rd party to authorize creation of a digital identity
- Logging of activity for auditing and trouble shooting purposes

Standards Support and Integration Considerations

Where possible, avoid non-standard technologies which require specifically integrated vendor components to be deployed.

Key Design Considerations

Technical Solutions

Case Studies

Specific Products

- Aegis
- Computing Associates
- Higher Ed Suite
- IBM
- Microsoft
- Novell
- Other Open Source Options
- Oracle
- Radiant Logic