Provisioning - Engine

Brief Description

A provisioning engine is responsible for synchronizing records from an IDMS and various target service providers (SPs). This synchronization usually considers a variety of eligibility rules to determine who should have access to what services for how long and with what authorizations.

Enterprise Provisioning refers to a model of a single IDMS with a master set of identities managing SPs within the virtual boundary of the enterprise (including, say, cloud services). *Federated Provisioning* refers to a model of multiple IDMSs sharing SPs across enterprise boundaries. The requirements of enterprise and federated provisioning are similar, but not identical.

Generic Functional Requirements

- Must support robust and timely data synchronization from the source IDMS, either via notification from the IDMS or extraction of state from the IDMS
- Should support message queues both for notifying external systems of changes and for receiving notification of changes from external systems

Standards Support and Integration Considerations

Support of SPML is desirable, however the number of IDMSs, Provisioning Engines, and SPs supporting SPML is low.

There are no standards for extracting data from the IDMS, which will likely require significant custom integration effort.

Key Design Considerations

See the Data Integration section for general principles that apply to this section as well.

The design of the source IDMS will likely influence how integration with the provisioning engine is designed. IDMSs capable of supporting change notification will likely push events to the provisioning engine, while those that do not will likely require the provisioning engine to have access to the IDMS' database.

Technical Solutions

A provisioning engine can be thought of a message switch, which accepts messages or extracts information from an IDMS and sends messages to SPs via real time notification, message queues, or batch extracts.