Person Data - Directory Services

Brief Description

One flexible model is to keep the IdM internal person directory separate from the IdM database of identity data. The latter is primarily used in support of authorization and related functions while the directory is ideally very data lightweight and used primarily for managing authentication functions internal to the IdM web SSO and access management components. In this case, one or more externally-facing directories may be provisioned from the IdM system and exposed for such business purposes as whitepage information about people, coarse application authorization needs, etc.

Generic Functional Requirements

1. Directories can provide authentication services to primary Web SSO systems such as CAS
2. Directories can be used to manage authentication policies around passwords
3. When used for application-based authorization, the directory must store attributes about users that can provide coarse role information which applications can consume as part of their authorization logic.

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

1. Commodity LDAP technologies such as:

- OpenLDAP