Authentication - Credential

Brief Description

Authentication credential stores include Kerberos KDC, LDAP, and relational databases. Web SSO protocols can rely on credentials from any of these stores.

Generic Functional Requirements

- Support for authentication mechanisms used for Web SSO.
- Support non-web-based authentication clients
- Support for credential policies such as complexity, age requirements, etc.
- Support for throttling and locking accounts based on repeated or total bad password submissions
- Support for multi-factor credentials
- Support for replication for redundancy; master-slave or multi-master
- Support (direct or API) for self-service password change

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

- web SSO technologies such as CAS or Shibboleth, integrated with credential policy controls such as those provided with OpenLDAP
- multi-factor technologies such as OTP tokens integrated with the web SSO technology

Case Studies

Specific Products

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