Scope and Principles

[OSIdM4HEteam:Meta]

Intent of this document:

- be the technical charter (for the overall activity) that is agreed to by initiative participants
- clarify technical scope of project
- state principles all current and potential workstreams should conform to
- demonstrate clear thinking and technical value to potential investors
- relate to OSIdM4HE Vision
- not require a glossary or functional model? but it uses all these technical terms ...

IAM: Institutional Infrastructure for Accountability and Expression

Persons, organizations, processes engage in online actions in myriad ways. Identity and Access Management (IAM) infrastructure supports a security-oriented institutional goal: accountability. Institutions want to ensure that online actors are accountable to institutional policies. This goal leads to infrastructure services for registering entities of all kinds, assigning credentials, supporting authentication and authorization, managing privileges, certifying compliance, etc. These services form the core of IAM.

As the information environment has grown, a second focus has emerged for IAM: enabling personal (and organizational) expression by facilitating the use of rich identity information across many systems. Institutions have an interest in having their affiliates "be themselves" using their institutional identity, within the institution and around the Internet. They have the corresponding interest in helping those with external identities use them in institutional systems. This goal leads to aspects of IAM services including user self-service, privacy controls, consent interfaces, federation, personal profiles, account linking, etc.

The twin organizational values of accountability and expression help define the scope and purpose of IAM services.

Solution Space Analysis

There are four primary functional areas in the IAM space: Identity Registries, Access Management, Authentication, and Provisioning.

Identity Registries: These services support the registration and lifecycle management of information about the entities that engage in online actions: people, processes, organizations, etc. Registries support constructs such as identifiers, accounts, credentials, and affiliations for a variety of entity types, where "person entities" tend to be most important.

Access Management: These services allow organizations to manage the capabilities of entities to make use of functions in online systems. These services support constructs such as groups, roles, and privileges that help access management processes scale.

Authentication: These services enable online actors to establish access to systems by securely proving their identities. Services also include management of authenticators such as passwords and public keys.

Provisioning: These services support the distribution of access-management-related information from IAM services to systems that rely on them, and conversely from source systems into IAM service systems.

As the importance and sophistication of IAM services increase, new functional areas are emerging. These include:

Information Presentation: These services make IAM information available to relying parties. Directory services are a traditional IAM component. More recently, web services, attribute services, event-based messaging, policy decision points, and other modes are becoming useful.

Personal Profile Management: These services allow persons, organizations, and other entities to maintain rich, highly-linked information about themselves.

Access Certification: These services monitor other IAM services and help to ensure that access management in practice is meeting organization policy goals.

New functional areas for IAM may come into view based on community experience.

Software solutions for IAM services, like any software, must also have:

Packaging: Software components must be available in forms to support the deployment lifecycle and a range of platforms. This includes installable packages, upgrade paths, etc.

Documentation: Software components must have good documentation, including installation and configuration, using APIs, etc.

Definitions/Concepts

Terms used in initiative documentation:

Components: A Component is a software package that is independently installable and operable to meet some IAM functional need.

Workstream: A Workstream is an administrative unit of effort, investment, and planning, devoted to producing one or more components.

Principles

Open-Source: All work produced by Initiative workstreams shall be licensed under compatible open-source licenses such as the Apache 2.0 License Apache License, Version 2.0 and the Educational Community License, Version 2.0 .

Standards-based: Use standards, promote standards, create standards, participate in standards development.

Enterprise-infrastructure-ready: externalized IAM, auditing, reporting, workflow, biz-continuity-enabled

Modular: Components are designed in a modular fashion so that adopters can, as much as possible, deploy a component without also being forced to deploy another OSIdM4HE component from the same or another Workstream.

Service-Oriented, Platform-Oriented: Access to all customer-facing Component functions is available via well-defined service interfaces callable from external programs. Components are designed to be Platforms that enable clients of IAM services (including other IAM components) to meet their IAM needs; this implies completeness of the service set as well as service orientation. When relying on other Components, Components use published service interfaces rather than project-internal interfaces.

Integratable:

Multi-implementation-friendly: In

Rely on existing components where possible

Enable management of policy as well as data: lifecycle, relationships,state transitions

Components and related products

Invested: KIM, Grouper, LDAPPCNG, potential new modules

Endorsed: Shib, CAS, OpenLDAP (other LDAPs), MIT Kerberos, simpleSAMLphp?

Commercial products are in the mix too ...