System Name: Feature List

Academic institutions are under pressure from customers and management alike to simplify, streamline, and automate identity management. System Name is an open-source, freely-available system designed to help academic institutions automate identity management processes. By implementing System Name, academic institutions can:

- Comply with auditing requirements – many institutions are required to be able to demonstrate that all access to systems is granted and removed in a timely manner;
- Improve security – when access to systems is granted and removed automatically, a disgruntled former employee or expelled student cannot wreak havoc on systems to which he/she previously had access;
- Enhance productivity – when customers are granted access to systems immediately upon (authorized) request, they are able to become productive more quickly;
- Improve customer service – when customers do not have to interact with IT staff to accomplish tasks, they have greater control over their computing experience; and
- Reduce costs and expand offerings – when identity management processes are streamlined and customers are able to take a broader range of actions without the involvement from IT staff, helpdesk staff are able to devote more time to other customer support issues, and other IT staff are able to reduce the amount of time spent handling day-to-day administrative tasks

System Name supports many features that are commonly required by academic institutions. Among these features are:

- Eligibility and lifecycle management
- Workflow
- Audit logging and reporting
- Identity correlation and resource reconciliation
- Entitlements management
- Self-service
- Delegated administration
- High availability and redundancy
- Scalability
- Modularity and open standards

Eligibility and Lifecycle Management

Before a resource can be provisioned for a customer, the customer must be eligible for the resource. System Name calculates resource eligibility based upon both roles and identity data. System Name also supports manual eligibility overrides (both positive and negative), so that a customer who falls outside the automated eligibility calculation can be accommodated.

System Name also manages identity lifecycles. That is, System Name will automatically provision and de-provision resources based on significant changes to an identity (such as graduation or start of employment).

With these two features, System Name provides institutions with the basic tools needed to automate all resource provisioning and de-provisioning.

Workflow

System Name allows workflow processes to be defined, such as the process of creating or removing resource objects. These processes are able to span long periods of time, and are able to be paused, resumed, or cancelled. With workflow capabilities, System Name can handle complex provisioning and de-provisioning processes.

Additionally, because not all eligibility is a simple matter of data, System Name allows for resources that require human approval through a workflow in addition to any automated eligibility calculation.

Audit Logging and Reporting

System Name keeps detailed records of each action taken through System Name, including who took the action and when. These logs provide auditors a way to ensure that the system is performing as intended, as well as a way to inspect anomalies.

System Name is also able to produce configurable graphical and tabular reports on these actions, as well as reports on basic identity and resource statistics, such as how many identities have access to a resource. An external tool may be used to create more detailed reports, and System Name provides a means for an external tool to access the audit logs. Because System Name provides comprehensive reporting capabilities, both administrators and auditors can quickly verify that access levels are appropriate.

Identity Correlation and Resource Reconciliation

System Name matches and links existing resource objects with identity records already in System Name based on some combination of attributes (e.g., shared common identifier, name/date of birth/SSN, etc). If a resource object does not match an existing identity record, System Name will create a new identity record and link the new record to the resource object. Once resource objects are linked to identities, System Name will monitor for changes in the identity that may affect shared data on a resource object (for example, name changes). If such changes are detected, System Name will propagate the changed data to any affected resource object.

System Name can also query for all resource objects on a given resource in order to verify links from those resource objects to identity records and to update any shared data on those resource objects. If System Name finds either resource objects that do not map to identities or resource objects that map to identities that are ineligible for that resource, the system can take corrective action and notify administrators of the errant records.

These two features together ensure that all resources are up-to-date and that any rogue accounts are identified and dealt with promptly.

Entitlements Management

The system manages entitlements as well as resource objects in order to provide a more comprehensive view of access across the institution. These entitlements may be granted based on roles and data and on workflow. System Name can also grant and revoke entitlements based on lifecycle events to ensure that entitlements are managed on the same basis as resource objects.

Self-Service

In order to improve the customer experience, System Name provides a complete set of self-service operations, including password management, access request, self-service password reset, and access request status. System Name also allows administrators to extend the set of self-service operations. These self-service options lead to a reduction of IT staff involvement in identity management processes, freeing them to work on other tasks.

Delegated Administration

Occasionally, administrator involvement on behalf of the customer is required – but sometimes the most appropriate person to respond to the customer is not a member

of the central IT group, but rather a departmental support person. System Name allows delegation of administrative rights on a fine-grained basis, so that a given delegated party can administer only a certain subset of identities, only a certain subset of access to resources, or a combination of both.

To reduce time spent by IT support staff when customers must contact support, System Name also provides a comprehensive set of utilities for service/help desk staff in order to enable them quickly to solve problems for customers.

High Availability and Redundancy

System Name is designed with high availability and redundancy in mind. While it is not required that a given instance of System Name be run in a highly-available and/or redundant manner, it is possible to do so with minimal configuration. Any reduction in downtime will reduce customer complaints, and System Name makes it simple for administrators to allow System Name to be fault tolerant.

Scalability

System name was designed to work in both small and large institutions, and is capable of dealing with at least one million identities and 100 resources. It is also capable of dealing with at least 50,000 actions (of all varieties) per day without any reduction in performance.

Modularity and Open Standards

System Name is based on open standards and specifications, such as SPML, LDAP, XACML, and WS-HT as much as possible to ensure broad compatibility with other systems. Besides being based on open standards, System Name is designed so that it is not prohibitively difficult to replace or extend any component of it, including downstream resource adapters. Each resource adapter is required only to implement a standard SPML interface to ease implementation of new resource adapters.

Glossary

provision (v)	the actual act of creating an object on a resource.
de-provision (v)	an invented word that means the actual act of removing an object from a resource
resource (n)	a system on which objects are to be created; e.g. an e-mail system, a calendaring system, or a research computing cluster
resource object (n)	the data and ownership information associated with a given identity's access to a resource; sometimes also known as an account
identity (n)	in the sense of computing, a digital collection of information that is specific to a given entity (person, application, machine, etc.)
eligibility (n)	whether the identity is authorized to have an object on a given resource; if the identity is authorized to have an object on a given resource, they are said to be eligible for that resource
entitlement (n)	a general thing for which an identity is authorized, including shared fine-grained authorization information not tied to a specific resource object
identity lifecycle (n)	the valid states and transitions between states for an identity; e.g. prospect to applicant to admitted to pre-matriculated to active student to alum.
identity record (n)	System Name's record of a given identity and its resource objects