Access Management Subcommittee Deliverables

The following information is intended to help guide the deliverable/s of the various subcommittees but should in no way constrain the outcomes of the groups.

Group Name: Access Management Subcommittee

Date

9/16/2011

Purpose of Group

Determine the requirements for an Access Management solution, perform a gap analysis of existing open source and commercial solutions and make a final recommendation to the OSIdM4HE group.

Gap Analysis

Glossary of Terms

Term	Definition

Requirements/Principles of the Chunk/Module

Namespace Requirements

Requirement ID	Requirement Source	Requirement Description	KIM	Grouper
NMSP_0100	Kuali	must allow for a concept called a Namespace which can be used for arbitrary categorization (system, functional category, etc)	Y	Y
NMSP_0110	Kuali	Namespace names must be unique	Y	Y
NMSP_0120	Grouper	Namespaces must support documentation metadata?		
NMSP_0130	PSU	Deep Namespaces (hierarchy?)	N	Y
NMSP_0140	PSU	Control of namespace nodes or folders is secured and can be assigned to distributed authorities as needed	Y	Y

Groups Requirements

What follows are requirements related to the groups portion of an Access Management solution. Cf notes from 10/24/2011 to amplify on some of these.

Requirement ID	Requirement Source	Requirement Description	KIM	Grouper
GRP_0100	PSU	The groups system shall support the establishment and maintenance of standing groups based on data from System(s) of Record (SoR).	N, but	Y
GRP_0110	PSU	The groups system shall support the establishment and maintenance of student class groups.	N, but	Y
GRP_0120	PSU	The groups system shall provide a distributed and delegated groups management function.	Y	Y
GRP_0130	PSU	The groups system shall provide a API and web service interfaces for accessing group information.	Y	Y
GRP_0140	PSU	The groups system shall support the publishing of groups information to other systems (LDAP, Active Directory, and so on).	N	Y
GRP_0150	PSU	The groups system shall support the creation, modification and/or deletion of groups and/or membership.	Y	Y
GRP_0160	PSU	The groups system shall support the construction of dynamic groups.LDAP in particular.	N	Y
GRP_0170	PSU	The groups system shall support nested groups.	Y	Y
GRP_0180	PSU	The groups system shall support groups that have an effective and/or expiration date.	Y	Y
GRP_0190	PSU	The groups system shall provide an end-user user interface for the management of groups.	Y	Y
GRP_0200	PSU	The groups system shall provide an auditing facility for all changes to groups/memberships.	Y (check Group Update Service)	Y

GRP_0210	PSU	The groups system shall provide a notification facility that user's/system's can subscribe to for group changes.	N	Y
GRP_0220	PSU	The groups system shall allow for attributes to be associated with a group (metadata).	Y	Y
GRP_0230	PSU	The groups system shall support the construction of a group from the members of other group(s) (group math).	N	Y
GRP_0240	Kuali	Maintenance of group members should be runtime configurable and changes should have the ability for workflow tied to them	Y	N

Roles Requirements

What follows are requirements related to the roles portion of an Access Management solution. Cf notes from 10/24/2011 to amplify on some of these.

Requirement ID	Requirement Source	Requirement Description	KIM	Grouper
ROL_0100	PSU	The roles system shall provide a facility for the management of roles.	Y	Y
ROL_0110	PSU	The roles system shall support three types of roles: basic, assigner (assigns users to roles) and stewards (assigns assigners to roles).	Y	Y
ROL_0120	PSU	The roles system shall provide an API and/or Web Services to access its facility.	Y	Y
ROL_0130	PSU	The roles system shall support the creation, modification and deletion of roles.	Y	Y
ROL_0140	PSU	The roles system shall support effective and expiration dates for a role.	Y	Y
ROL_0150	PSU	The roles system shall support permissions and/or limits associated with a role.	Y	Y
ROL_0160	PSU	The roles system shall support the publishing of role information to other sources, for example LDAP.	N	? (ask Jimmy)
ROL_0170	PSU	The roles system shall support the concept of a role proxy where a person is given access for a limited period of time.	Y	Y
ROL_0180	PSU	The roles system shall support a hierarchy of roles, which enables the reuse of roles.	Y	Y
ROL_0190	Kuali	Roles aggregate Permissions	Y	Y
ROL_0200	Kuali	Roles are not limited to a single Namespace and can span across them (i.e. a Role can allow for actions in Namespace A and Namespace B)	Y	Y
ROL_0210	Kuali	Roles are tied to Principals or Entities or Groups, and any Principals or Entitites or Group with a certain Role has the ability to perform the actions designated as Permissions that are associated with a Role	Y	Y
ROL_0220	Kuali	A Role must be able to be scoped or qualified such that one can apply it to a specific context (eg, Fiscal Officer Role scoped to Account XYZ)	Y	Y
ROL_0240	Kuali	A Qualified Role must be maintained with the ability for workflow approvals	Y	N

Permission Requirements

Requirement ID	Requirement Source	Requirement Description	KIM	Grouper
PERM_0100	Kuali	Permissions represent fine grained actions that a Person or Group can perform in a system (i.e. canEdit, canSave, etc)	Y	
PERM_0110	Kuali	Permissions are scoped to a Namespace and cannot cross Namespaces	Y	
PERM_0120	Kuali	Permissions can be given to many different Roles	Y	

Attributes Requirements

What follows are requirements related to the attributes portion of an Access Management solution

Discussion 11/3/2011: Neither KIM nor Grouper focus on being attribute service providers, but they provide access management capabilities to applications that can be based on person attributes. However, Grouper's LDAP provisioning connector can provision person attributes based on their group memberships, and the GrouperDataConnector for shibboleth allows a shib IdP to express attributes as a function of group memberships. Both KIM and Grouper support attributes on groups and Grouper support attributes on other types of objects and KIM manages Principals/Entities with attributes.

Requirement ID	Requirement Source	Requirement Description	KIM	Grouper
ATT_0100	PSU	The system shall provide an attribute services. Attributes can either be single-valued or multi-valued.	Y (check on multi-valued attributes)	Y
ATT_0110	PSU	The system shall support public and sensitive (limited access) attributes.	Y	Y
ATT_0120	PSU	The system shall support official and user-modifiable person attributes.	N/A	N/A
ATT_0130	PSU	The system shall provide Web Services to access attributes.	Y	Y
ATT_0140	PSU	Attributes from eduPerson, inetOrgPerson and orgPerson objectClasses shall be available for use in federating applications.	N/A	N/A

Policy Engine Requirements

What follows are requirements related to the policy engine portion of an Access Management solution

Requirement ID	Requirement Source	Requirement Description	KIM	Grouper
POL_0100	PSU	Granting and removal of access shall be performed automatically according to defined business rules.	Y, KIM includes a number of role type implementations for common business rules	Y
POL_0110	PSU	The system's policy engine shall be high performing and flexible enough to allow for a variety of rules.	Vague. Works for existing customer deploys.	Vague. PDP is new, not much field experience yet.
POL_0120	PSU	The system's policy engine shall be accessible from either a Web-based GUI or Web Services with appropriate access controls.	Y	Y
POL_0130	PSU	The system's policy engine shall allow for searching of existing rules for possible reuse.	Y, roles & permission objects can be reused	Y, roles & permission objects can be reused
POL_0140	PSU	The system shall support a centralized policy engine responsible for managing and evaluating policy rules (PDP).	Y	Y
POL_0150	PSU	The system shall support a policy enforcement point (PEP).	N, but apps written using Kulai Nervous System have built-in PEPs.	N

Auditing Requirements

What follows are requirements related to the auditing portion of an Access Management solution

Requirement ID	Requirement Source	Requirement Description	KIM	Grouper
AUD_0100	PSU	The system shall support the periodic review of a user's privileges as defined by policy.		
AUD_0110	Kuali	A support desk needs to easily be able to see what access and permissions a person has and why they may not be able to perform a task they need to	N	

Enterprise Requirements

What follows are requirements related to the enterprise aspect of an Access Management solution

Requirement ID	Requirement Source	Requirement Description	KIM	Grouper
ENT_0100	Kuali	Service interfaces must be defined for all API interaction	Y	
ENT_0110	Kuali	All services must be invoke-able via Java and have XSD/WSDL for SOAP/XML-RPC invocation	Y	
ENT_0120	Kuali	All services must be swappable with custom implementations (services must interact via service api's and never directly against anothers data, ex: role service can't read permission tables)	Y	

PACCMAN Requirements

What follows are requirements related to the enterprise aspect of an Access Management solution

Requirement ID	Requirement Source	Requirement Description	KIM	Grouper
PAC_0100	B-2	The system shall support the ability to transfer access rights to another user.		
PAC_0110	B-3	The system shall support time-limited delegation of application privileges from authority to designee with a pre-defined time limit.		
PAC_0120	B-14	The system shall support point in time auditing of permissions.		
PAC_0130	B-15	The system shall support the automatic recalculation of privileges based on granular changes in multiple affiliations.		
PAC_0140	A-8	The system shall support granting time-limited access previously granted automatically via group membership to a single subject.		
PAC_0150	L-2	The system shall support federated identity coupled with federated group membership for shared access to resources.		

Scope

- Groups
- Roles
- Attributes
- Enterprise

Project Definition

- Resources Needed, Outcome Expected, Timeline

Recommendations: