Identity Management Requirements

Table of Contents

1 OVERVIEW 3

1.1 Approach 3

1.2 Architectural Goals and Constraints 3

1.3 Business Requirements 3

1.4 High Level Business Requirements Overview 3

1.4.1 Architecturally Significant Requirements 3

1 Overview

Identity Management requirements for a large non-profit organization are presented in this document. This non-profit has two business units called chapter and biomedical. Chapter is mainly responsible for disaster relief and biomedical is mainly responsible for blood collection, storage and supply.

1.1 Approach

Architecture and design should include component model, sequence diagrams and any other appropriate models.

1.2 Architectural Goals and Constraints

- Enterprise has already invested in many of the components of identity management like LDAP, which will be reused where possible. Biomedical side uses mainly LDAP for authentication/authorization.
- Active Directory is being used on chapter side and will continue to be primary source of user data. Architectural solution proposed should account for integration with active directory.
- ERP systems are also being used on chapter side to handle user authentication and authorization. Architectural solution must integrate with ERP
- A J2EE product is being used for training. Identity management solution must also integrate with training product.
- Architecture has to be generic and flexible

1.3 Business Requirements

The business requirements for reference architecture are generic in nature. The following are the typical requirements for any project that wants to implement identity solution. Individual project must build on the following requirement/use cases to make the requirement more specific to that project.

1.4 High Level Business Requirements Overview

Business requirements consist of providing user authentication and authorization based on Active Directory, LDAP and single sign on technologies. Different business units in ARC do authentication and authorization differently right now. There needs to be a common authentication and authorization model. Microsoft Active directory will act as a primary source of user data. User authentication needs to be reconciled across business units that use peoplesoft, siebel and learning management system called plateau (J2EE Application).

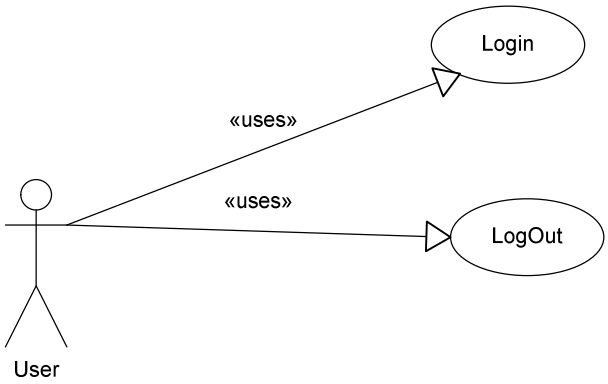
1.4.1 Architecturally Significant Requirements

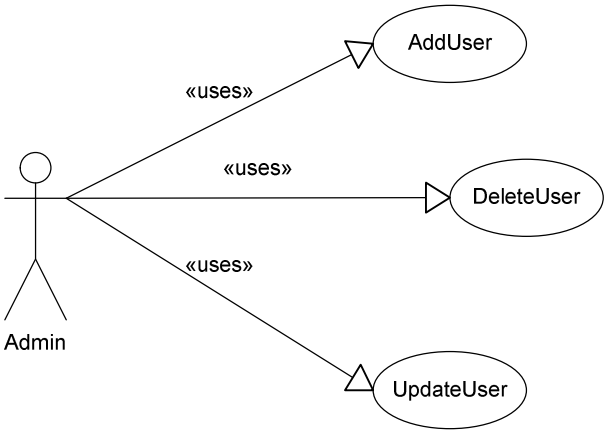
The following use cases have been identified for identity management

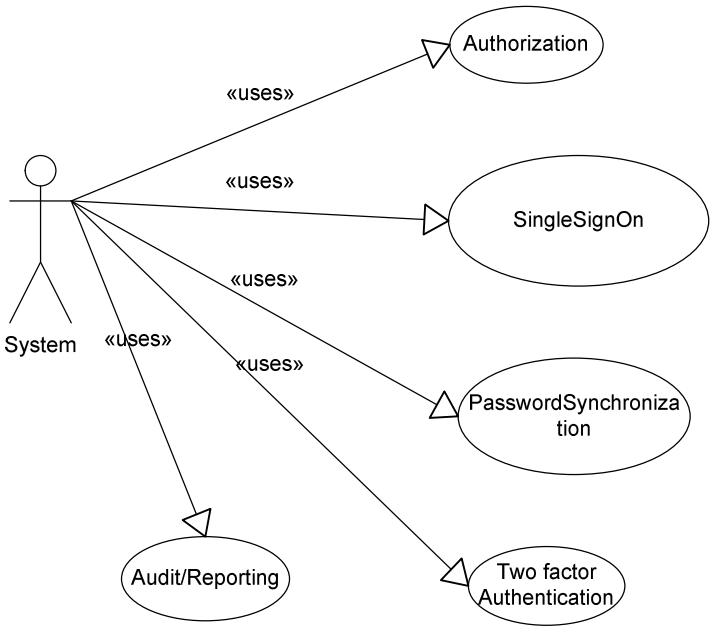
UseCaseName	Description
LogIn	User chooses to log into the system
LogOut	User logs out of the system
SingleSignOn	User log into one system and is granted access to all the systems
Password Synchronization	Password is synchronized across all the systems
AddUser	User is added to different systems
DeleteUser	User is deleted in different systems
UpdateUser	User information is updated between LDAP and active directory

Authorization	System checks if the user has needed permissions to access the services requested
Two factor Authentication	Token based authentication where the user enters the token and pin. Token is usually generated by a token card in possession of the user
Audit/Reporting	Auditing and reporting on user activity

Use cases will be identified for specific projects as decisions are made to implement identity management. The following is the use case diagram.


Login
«uses»
«uses»
LogOut
User


AddUser
«uses»
«uses»
DeleteUser
«uses»
Admin
UpdateUser


Authorization
«uses»
«uses»
SingleSignOn
«uses»
«uses»
System
«uses»
PasswordSynchroniza
tion
Audit/Reporting
Two factor
Authentication

Identity management

Addendum to problem 3 for the 2005 DesignFest®

This addendum was written by the DesignFest® committee after problem submission had closed. Responsibility is with the committee not with the problem author.

The committee wants to add some complexity to the problem in the form of some restrictions, to be added to the types of information specific users can access. This adds to the complexity of the design, but we feel it is more attuned to typical security needs of organizations. Also it was the feeling of the committee that it would prevent groups building a system out of of the shelf components to easily. Groups are free to add or ignore these additions.

The additions for this would be:

1.2: Data available is restricted to authorized users. Users are granted access to specific types of data, and data repositories not matching any of a user's authorization codes will not be displayed to that user.

1.4.1:

UseCaseName	Description
AddAuthorizationType	Authorization to access a specific type of data is added to the user's User Authorizations List
RemoveAuthorizationType	Authorization to access a specific type of data is removed from the user's User Authorizations List
DisplayAuthorizedData	User who has successfully logged in is shown the data repositories available to their authorization type(s)