Centralized Directory Services 
and Accounts Management Project

Rob Murawski 
University of Pittsburgh 
Computing Services & Systems 
Development 
717 Cathedral of Learning 
Pittsburgh, PA 15260 
(412) 383-9637 
rsm4@pitt.edu

1. INTRODUCTION

The Information Technology (IT) field and its constituent technologies continue to develop and mature at a rapid rate. Nowhere is this change more prevalent than in the security of IT resources. Emerging authentication technologies, combined with forthcoming directory service solutions, provide unique opportunities for developing and integrating comprehensive solutions to central directory services and single sign-on environments. The University of Pittsburgh has reviewed its computing account structure and how the system manages access to an array of IT assets. Account discrepancies and anomalies led to the need to develop a progressive solution, reflecting advances in security, network and end-user technologies. In 1998 the University assembled a team to design and implement a comprehensive central directory and account system.

The Centralized Directory Services and Accounts Management Project can be broken into four major components:

1. Centralized Directory Services. This component is the full listing of all University of Pittsburgh-affiliated individuals and allows an authoritative listing of all individuals at the University of Pittsburgh.

2. Web-based Tools. The web-based user and administration tools need to interface with the directory, authentication systems, and other directory information.

3. Single-Sign-On and Authentication. This component handles the authentication of users and allows for the single-sign-on.

4. Data Cleansing. A data-cleansing project will be ongoing during all of the migration efforts. This component ensures that each account maps to a person affiliated with the University of Pittsburgh and any other accounts have justification.

The presentation will report on the goals of the project as proposed, and will compare these items to the final implementation. Significant time will be devoted to strategies, design considerations, technical specifications, hardware/software parameters and the implementation process, with particular attention given to lessons learned. A portion of the presentation will focus on future functionality and additional features that are scheduled for long-term implementation.

Secondary Goals

1. development of the EDUPerson 
2. adherence to Instructional Management Systems (EDUCAUSE) standards 
3. explore medical middleware issues 
4. generic — how is this expressed in the core deployment? 
5. specific — what medical data structures need integration into campus environments? 
6. outreach to encourage other institutions 
7. research options for authorization services 
8. evaluate new tools and technologies

Keywords 
Single sign-on, directory service, public key infrastructure, authentication and security.

2. BACKGROUND

The Information Technology (IT) field and its constituent technologies continue to develop and mature at a rapid rate.
Nowhere is this change more prevalent than in the security of IT resources. Emerging authentication technologies, combined with forthcoming directory service solutions, have required the University of Pittsburgh to review its computing account structure and how the system manages access to an array of IT assets. Several decades of accumulated account discrepancies and anomalies led to the need to develop a progressive solution that would reflect substantial advances in security, network and end-user technologies. In late 1998 the University of Pittsburgh assembled a team to plan the design and implementation of comprehensive central directory and account system.

The Central Directory Services and Accounts Management team was given seven objectives:

10. Design and implementation of enterprise directory services
11. Integration of charging mechanisms
12. Development of account extension policies and privileges
13. Implementation of enhanced reporting functions
14. Design and implementation of improved account support mechanisms
15. Integration of digital certificate technology

The presentation will outline the strategies, design considerations, technical specifications, hardware/software parameters and the implementation process of the new account management systems and the centralized directory services.

3. REFINEMENT OF GOALS

Refinement of the original set of project objectives produced the following project goals:

1. Single-Sign-On (SSO) across all University of Pittsburgh supported platforms. This allows the use of a single username and password to access shared file space, e-mail, restricted web pages, lab machine usage, and any other service the University of Pittsburgh may implement. The SSO solution should be robust and extendable for future systems.

2. Single account per user. This changes the person to account paradigm from a many-to-many relationship to a one-to-one relationship. Currently, many accounts are “group” accounts since more than one person uses them. This makes accountability impossible for these accounts. Other people have more than one account that makes accounting for different job functions easy, but difficult to maintain multiple passwords, file spaces, logon rights, and other items which are included with the account. This paradigm change requires changes in thinking on the part of the end-user: shared accounts will not exist, instead shared areas can be created. Accounting will need to be done by ‘instances’ or ‘partitions’ of a user account.

3. Web-based administration. This allows any administrator to create, approve, request, or delete accounts via a platform-independent web page. The web-based administration requires no additional software on the workstation.

4. Web-based user tools. This allows users to easily view and change their account information. Such tools include, but are not limited to, viewing system quotas, system usage information, changing passwords, and changing the advertised e-mail address.

5. Enterprise directory services. Someone should be able to query an enterprise-wide directory to find any public information about a person. Additionally, certain authenticated users may be able to access more information on certain users.

6. Departmental access to authentication. In order to achieve a pure single sign-on as well as provide for University security, departments should be able to authenticate to the University of Pittsburgh central authentication system.

Given these design goals, the Centralized Directory Services and Accounts Management project must consider the following:

Current authentication systems in place at the University of Pittsburgh. These systems must be in place to allow a transition from the older system to the new system.

Current business practices at the University of Pittsburgh. These business practices must be examined and possible administrative
actions will need to be taken to adjust some of the business practices.  

Minimizing user disturbances. The users should experience little or no disruption during the transition to the new system.

The Centralized Directory Services and Accounts Management Project can be broken into four major components. In order of dependencies, they are:

1. Centralized Directory Services. This component is the full listing of all University of Pittsburgh-affiliated individuals. This database is needed to allow an authoritative listing of all individuals at the University of Pittsburgh.

2. Web-based Tools. The web-based user and administration tools need to be written to interface with the directory, authentication systems, and other directory information.

3. Single-Sign-On and Authentication. This component handles the authentication of users and allows for the single-sign-on.

4. Data Cleansing. A data-cleansing project will be ongoing during all of the migration efforts. This component ensures that each account maps to a person affiliated with the University of Pittsburgh and any other accounts have justification.

4. GOALS OF THE CENTRALIZED DIRECTORY SERVICES

The Centralized Directory Services portion of the project has the following goals:

1. Provide a centralized listing of all University of Pittsburgh-affiliated students, staff, and faculty.

2. Allow directory lookups to find public information on any persons listed in the directory.

1.1 REQUIREMENTS TO COMPLETE THE CENTRAL DIRECTORY SERVICES

The Centralized Directory Services portion of the project requires the following hardware components:

1. Two redundant servers for storage and access to the actual CDS database. These servers should exist in physically separate, but physically secure, locations on campus. Because this service will be controlling the account creation/deletion of the authentication systems, a single point of failure will be detrimental to the function of the University. By having two redundant servers, the single point of failure is removed.

2. Public interface server to access the CDS information. This server will allow LDAP-based searching of the CDS information. The CDS Hardware Team recommends that this interface run on one of the above CDS servers.

The Centralized Directory Services portion of the project also requests the following hardware for optimum performance:

1. Network security equipment, such as firewall hardware, to protect the database servers. This hardware will filter out unauthorized network packets and improve the security of the database.

2. Network encryption equipment, such as a hardware virtual private network. This allows network traffic between the two database servers to be encrypted as it travels over the network. This will prevent unauthorized users from viewing any confidential account information between the two database servers. This technology could also be extended to allow the system administrators to use encryption to access the database and system.

Additionally, the following software will be required by the Centralized Directory Services portion of the project:

1. Oracle server software for the two database servers. Oracle replication will be utilized to replicate data between the two servers.

2. LDAP and web server software for the user interface.

5. GOALS OF THE WEB-BASED USER TOOLS

The Web-Based User Tools portion of the project has the following goals:

1. Provide an intuitive environment for users to self-manage their account.

2. Provide on-line help to support the account management environment.

1.1 REQUIREMENTS TO COMPLETE THE WEB-BASED TOOLS

The Web-based Tools portion of the project requires the following hardware components:

1. Two Intel-based servers. Two web server machines are required to support the web site. Given the critical role of this web site, redundant servers will ensure 100% user availability. Much of the functionality can be created with Active Server Pages (ASP). ASP excels at creating web pages that interface with a database and is easy to support.

The Web-based Tools portion of the project requires the following software components:
1. Server operating system software. Windows NT Enterprise Edition is the server operating system. This includes the web server software and the Windows Load-Balancing software.

2. Web Development software. Microsoft Visual InterDev, an integrated development environment (IDE), will be used to create ASP code. Microsoft Visual SourceSafe will be used as the version control system software.

The Web-based Tools portion of the project requires the following additional components:

1. Development workstations.

2. Firewall hardware to protect the web servers. This hardware would filter unauthorized network packets and allow administrative access only to authorized individuals. Only network traffic destined for the web-server would be passed. This can use the same firewall hardware as used in the CDS system.


6. SINGLE-SIGN-ON GOALS

The Single-Sign-On portion of the project has the following goals:

1. An authentication mechanism that is extensible must be developed for the University’s single-sign-on. It is proposed that the new CDS system allow feeds to different authentication systems to provide for an easy transition to newer authentication systems.

2. The ultimate goal of the authentication project is to provide a single authentication mechanism that can be used to provide access to all University computer resources, including departmental resources as well as centrally maintained systems.

3. The authentication mechanism must be flexible enough to allow authentication via different types of credentials (such as username/password combinations, smart cards, and/or digital certificates.)

4. The authentication mechanism must be able to accommodate future changes in technology, such as enabling authentication against different “back end” databases.

5. The authentication mechanism must be able to co-exist and integrate with existing authentication methods to prevent disruption to the end-user’s environment.

1.2 REQUIREMENTS TO COMPLETE THE SINGLE-SIGN-ON

The Single-Sign-On portion of the project requires the following hardware components:

1. Novell NDS servers are required for building the centralized NDS tree. A minimum of two high-end servers is requested with an ideal number being four servers for best load balancing and redundancy.

2. Workstations for management of the NDS tree. These workstations can be workstations already owned by CSSD. Each person managing the tree will require a workstation.

3. Two Windows NT 4.0 servers for allowing authentication of the Windows NT-based services.

4. Various NDS servers distributed throughout the organization to maintain authentication services “close” to the end users.

The Single-Sign-On portion of the project requires the following software components:

1. Novell NetWare/NDS licenses to cover the required number of servers

2. NDS management software such as DS Expert from NetPro.

3. Two copies of NDS4NT software for Windows NT operability with the NDS tree.

The Single-Sign-On portion of the project requires the following additional components:

1. Sufficiently skilled network administrators to manage the various servers.

2. Programming expertise to integrate other authentication schemes to use NDS.

7. GOALS OF DATA CLEANSING

The Data Cleansing portion of the project has the following goals:

1. Each account holder will have one and only one primary network account

2. Accounts that fall outside the primary holder/account relationship will be categorized as sponsored, i.e. departmental, guest with a required primary and optional secondary account sponsor.

3. To the greatest extent possible inactive and non-affiliated accounts will not be migrated.

4. The accounts migrated from the CAP system to CAMS will be “enabled” as defined by the hosts currently fed by CAP.
CAP will accurately reflect account status as defined by the hosts.

1.1 REQUIREMENTS TO COMPLETE THE DATA CLEANSING

1. The Data Cleansing portion of the project will use existing hardware and software resources of CSSD. No additional hardware or software will be requested at this time.

8. OUTCOMES

The Centralized Directory Services and Accounts Management Project is currently underway and following the timeline established by the project plan. The full implementation date is scheduled for mid-summer of 2000. The presentation will report on the goals of the project as proposed, and will compare these items to the outcomes and results of the final implementation. Significant time will be devoted to the obstacles and barriers to the project, with particular attention given to lessons learned. A portion of the presentation will focus on future functionality and additional features that are scheduled for medium to long-term implementation.