

Identity and Access Management Service Charter

Executive Summary

One of the goals of the Office of the CIO (OCIO) is to enhance, promote, and support the effective enterprise-wide use of information that supports MUSC's mission. Computer systems and applications throughout the MUSC enterprise have a common need to manage their users and to electronically identify their users. Because the Infrastructure Division of OCIO-Information Services maintains the core technology infrastructure that supports these systems, the Infrastructure Division seeks to meet these common needs by centrally providing identification services, authentication services, and authorization services. Collectively these services will be referred to as Identity and Access Management (IdAM) services.

Identity and Access Management services will benefit system administrators, security administrators, and users. From a system administrator and security administrator's point of view, utilizing the Identity and Access Management services means that more of the account provisioning, de-provisioning and access management processes can be automated via business rules. Also, the identity and access management foundation doesn't have to be built from scratch for each system or application. From a user's perspective, there is less red tape, i.e. less forms and fewer points of contact, required to get setup for the computer systems and applications necessary for their job functions. Also, password management becomes more straight forward for the user, i.e. choosing a password, changing a password, and resetting a password all become straight forward processes synced across most of their applications and systems.

Scope

As defined below, Identity and Access Management services include the metadirectory and those physical directories deemed to have enterprise significance. The interface between the core business systems of record and the metadirectory will be centrally supported. Also, the Person Registry Application will be centrally supported as the means by which non-core sources of a person's identity information feeds into the metadirectory. Similar to the person object, the scope of Identity and Access Management services will be expanded to include non-person objects. For example, services will be provided for System Registry. Services will be provided for non-person objects on a case by case basis as resources permit.

The primary purpose of the Identity and Access Management services is to supply information in standard formats and protocols so that systems and applications can utilize it to identify, authenticate and authorize users. In order to develop procedures for applications and service platforms to integrate with Identity and Access Management services, OCIO-Information Services will integrate several key systems (KEANE, OACIS, Remedy, and Advanced Point of Care Systems (APOC)). It is expected that individual system administrators will follow the procedures and integrate their systems with the Identity and Access management services. Requests for further assistance from the Infrastructure division of OCIO-Information Services will be handled on a case by case basis.

Identity Management Concepts and Terms

The core of Identity Management services will be an Enterprise Directory. The Enterprise Directory consists of a Metadirectory and one or more physical directories. The Metadirectory consists of the Person Registry and documented Business Rules (the processes and logic governing how systems of record and other sources interact with the Enterprise Directory and how consumer systems and applications interact with the Enterprise Directory). Some of the other sources will be registries in their own right, such as System Registry. Several physical directories are already centrally provided, such as the MUSC LDAP "white pages" service that supports email and the AuthLDAP service that supports authentication of [MUSC Network Account \(MNA\)](#) users. While these directories were designed to perform very specific, narrow functions, the scope of the Enterprise Directory will be much broader: it will be designed to meet both the immediate needs of existing applications and the future needs of a broad range of "directory-enabled" applications and services.¹

¹[Metadirectory Practices for Enterprise Directories in Higher Education](#) Copyright © 2002 byUCAID and/or the respective authors October 2002

Identity and Access Management Service Charter

A registry is the system in which a resource's identity possibly obtained from multiple source/owner systems is resolved. Registry data is often housed in a relational database². The resource in question can be a person, a system, a printer, a room, etc.¹

“An identifier is a function that maps real-world subjects into name or character strings, so that distinct subjects have distinct strings. A real-world subject may be a person, an object (for example, a printer or a file), a group, or a department. A real-world subject can have multiple identifiers. For example, a person may have a Social Security number, an email address, user ids on several systems, a network ID, and others.”³ Thus the Enterprise Directory will provide those identifiers deemed useful to the MUSC Enterprise. Since a real-world subject may have multiple identifiers, the Enterprise Directory will also relate the various identifiers to a single global identifier. As indicated in the IdAM pyramid below, Identification is the foundation of IdAM Services.

“Authentication is the process of establishing whether or not a real-world subject is who or what its identifier says it is.”¹ The Enterprise Directory can relate an identifier, such as a username, with its authenticating credentials, such as a password. Use of an authentication directory service such as may be provided by LDAP, reduces the number of passwords a user needs to remember. A user may have to repeat the login process for each application he uses, but at least the username and password are the same each time. In order to support single-sign-on, whereby a user logs in only once per session, regardless of how many applications he accesses, a technology designed specifically for authentication, such as Kerberos may be provided. A Kerberos realm will be another consumer of metadirectory information. Note in the IdAM pyramid, the authentication layer resides on top of the identification layer; that is, in order for the username to be provided in the Enterprise Directory, it must be associated with the global identifier provided by the Enterprise Directory. Thus rules governing the provisioning and disabling of authentication credentials are based on the identification layer of the Enterprise Directory.

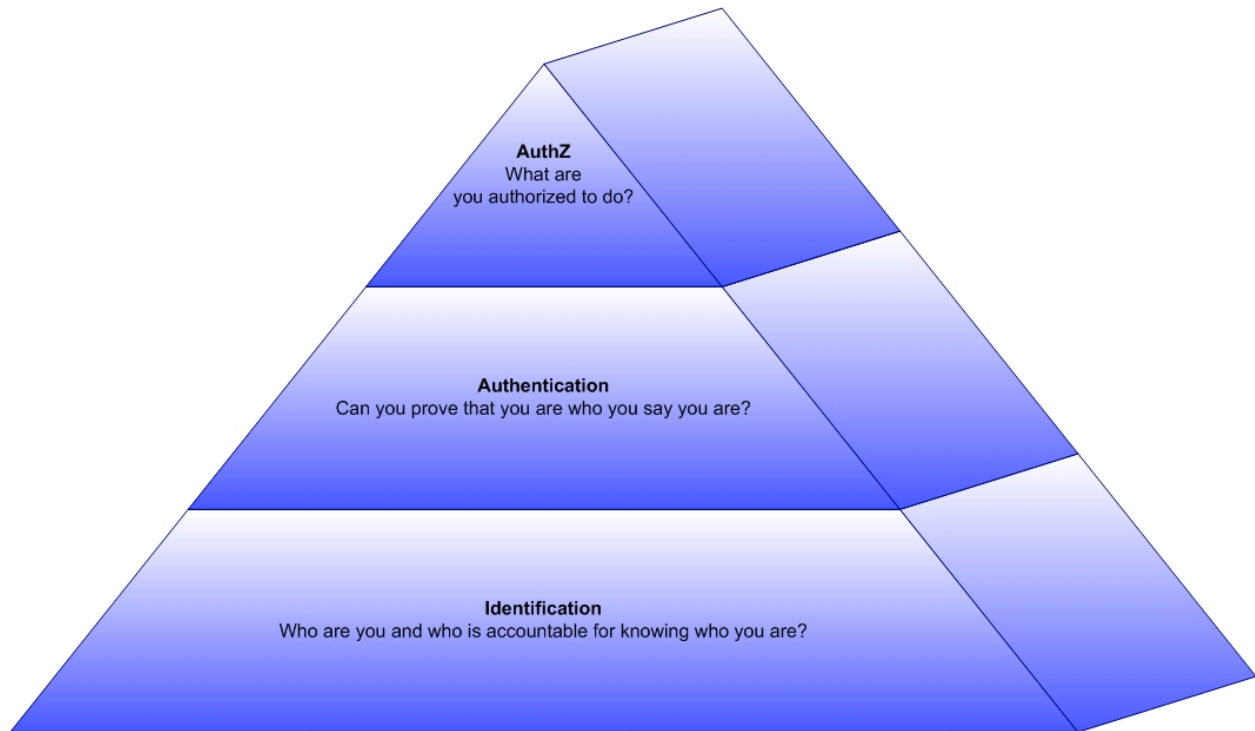
“Authorization indicates what an identifier, properly authenticated, is permitted to do with a networked object or resource.”⁴ Although a user usually asks for authorization first, i.e. “Please give me access to do thus and so”, the authorization layer is actually the top of the pyramid, specifically on top of the authentication layer, in that the user must be properly authenticated before being authorized to do anything. In addition to identifiers, the Enterprise Directory may contain other attributes of a real-world object, such as group membership. These attributes can be utilized to make authorization decisions.

²[Identifiers, Authentication, and Directories: Best Practices for Higher Education](#) Internet2 Middleware Initiative
May 9, 2000

³[Internet2 Identifiers page](#) © 1996 - 2005 [Internet2](#) - All rights reserved

⁴[Appendix: PASE Terms](#) Presentation by Keith Hazelton, Senior IT Architect, Univ. of Wisconsin-Madison
Member, Internet2 Middleware Architecture Comm. for Education (MACE) Internet2 Fall Member Meeting,
Indianapolis, Oct. 15, 2003

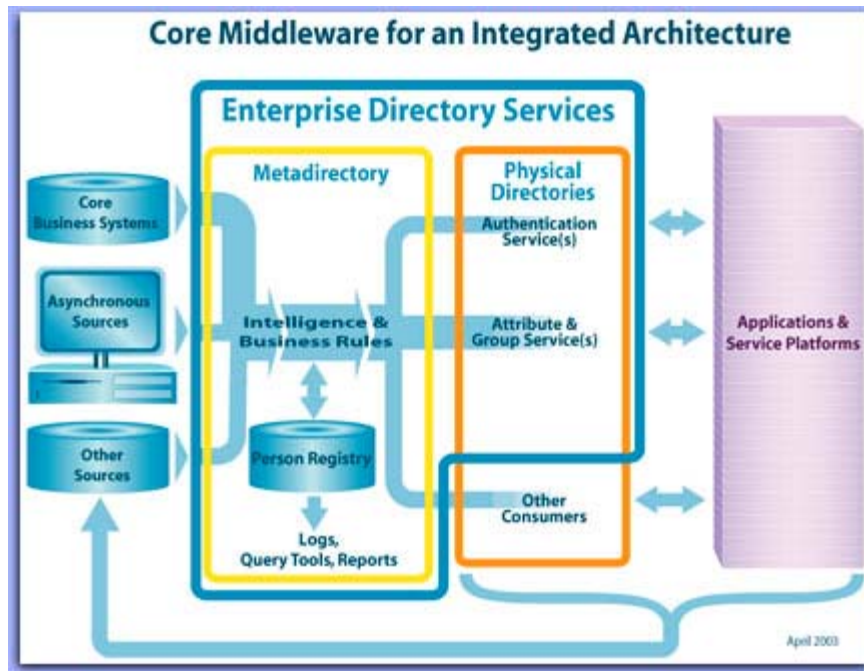
Identity and Access Management Service Charter



Another common need of systems and applications is to communicate with users. Thus the Enterprise Directory will contain contact information, such as phone numbers, mailing addresses, and e-mail addresses. Often, the systems of record are not the authoritative sources of such data, so other sources will feed the Enterprise Directory.

Identity and Access Management Service Charter

The NMI-EDIT reference diagram of the resulting architecture is as follows⁵:

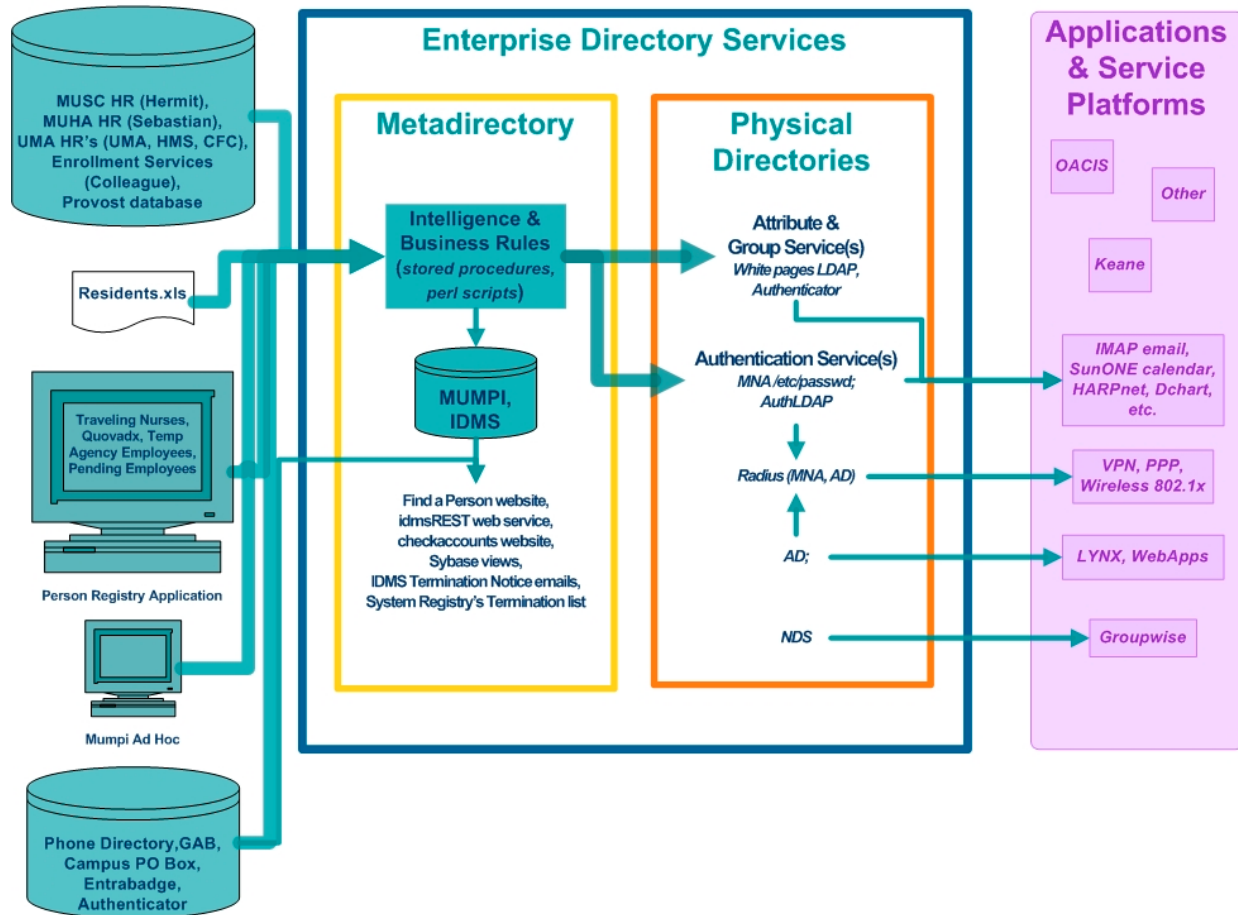


Some components of the Identity and Access Management service infrastructure already exist. A pair of relational databases already exists that are fed person identity information from our core business systems of record. The relational databases are MUMPI (MUSC Master People Index) and IDMS (Identity Management System). MUMPI is currently being fed from the core human resource business systems of record: HERMIT for MUSC University, Sebastian for MUHA, all 3 instances of UMA/CFC INFINIUM system, Colleague for Enrollment Services, and the Provost database. The Person Registry application is already in production, although it is currently largely limited to MUSC University and MUHA HR personnel who use it to register pending employees and temporary agency employees. Person Registry is also currently used to register Traveling Nurses and Quovadx personnel. There are also other existing sources of person attributes: Phone Directory database, GAB (Global Address Book), Campus PO Box database, and Entrabadge. The Phone Directory database and GAB feed the white pages LDAP, but these attributes are not currently stored in MUMPI or IDMS. Several query tools and "reports" are currently provided: the [Online Directory](#) website, the [idmsREST](#) web service, [checkaccounts](#) website, various database views, IDMS Termination Notice emails, and [System Registry's Termination list](#). Several physical directories and other services exist for authentication services: AuthLDAP, MNA's etc/passwd, Radius, and Microsoft Active Directory. AuthLDAP electronically checks against GAB and MUMPI, but Microsoft Active Directory does not. Microsoft Active Directory contains authorization information, but again does not electronically check against GAB or MUMPI. An authorization tool exists that is directly connected to MUMPI and GAB; it was inappropriately named Authenticator. Some Applications and Service platforms already take advantage of the existing Identity and Access management services, such as IMAP email, SunONE Calendar, HARPnet, Dchart, several other web applications, a host of internal websites, LYNX, WebApps, and VPN. See Appendix B for for a list generated from System Registry. The state of today's IdAM Service Architecture can be diagrammed as follows.

⁵Core Middleware for an Integrated Architecture diagram as published in [The Enterprise Directory Implementation Roadmap](#) Copyright © 2003 by Internet2 and/or the respective authors December 2003

Identity and Access Management Service Charter

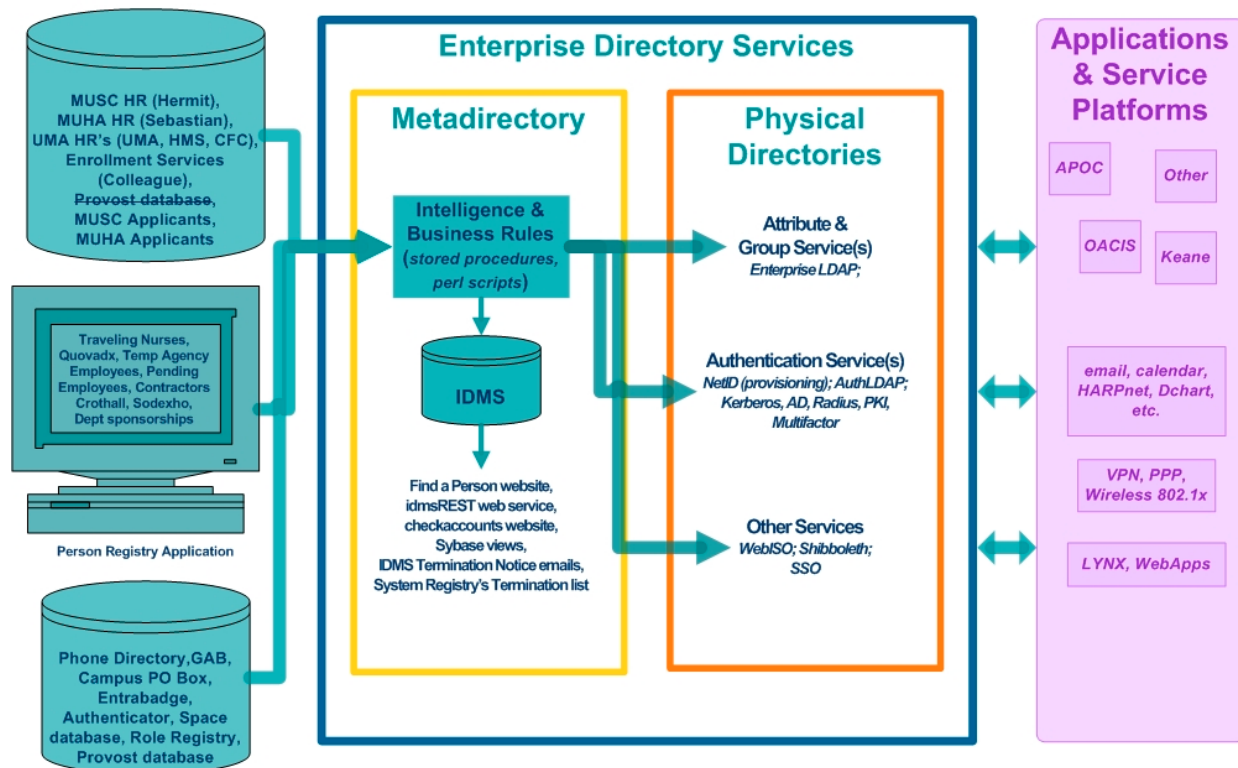
Today's Identity and Access Management Service Architecture



The future Identity and Access Management Service Architecture will expand upon many of the existing components. The existing core business systems of record will continue to feed the metadirectory. Use of the Person Registry application will be expanded to include all non-core sources of people, such as Crothall, Sodexo, and other contractors, all temporary employment agencies, and department level sponsorships. In addition to expanding on existing components, the existing components will be strengthened or replaced with stronger components. For example, the existing interfaces, stored procedures and scripts will be reworked into a coherent set of business rules. The MUMPI and IDMS relational databases will be merged into one database. The services provided by physical directories will be expanded to include authorization and more attribute and group services. Significantly, the Microsoft Active Directory will be synced with the Enterprise LDAP and AuthLDAP. To reduce confusion, the resulting account will be known as the NetID. The authentication services offered will be expanded to include Kerberos, PKI and multifactor authentication. Other services offered will include WebISO, SSO, and Shibboleth. Those applications and service platforms that currently utilize AuthLDAP or Microsoft Active Directory will migrate easily into the future IdAM Service Architecture. Other legacy applications, such as OACIS and KEANE will have to be integrated with the architecture. The future Identity and Access Management Service architecture can be diagrammed as follows.

Identity and Access Management Service Charter

Future Identity and Access Management Service Architecture



Deliverables

- Person Registry (the database component of the Metadirectory)
- Implementation and maintenance of the Business Rules that control the Metadirectory (system of record import processes, identity matching rules, sponsorship termination rules)
- Creation and distribution of centrally provided identifiers (publicly visible identifier - PVI)
- Other object directories, such as a directory of Systems published from System Registry.
- Implementation and maintenance of Physical Directory Services (MUSC LDAP White Pages, AuthLDAP, Enterprise LDAP, Kerberos authentication service)
- Directory replications (redundancy of the Enterprise LDAP for performance or specialized purposes)
- Provisioning enterprise consumers of directory information (e.g., Microsoft Active Directory)
- Documentation of policies and procedures for consumers of directory information
- Technical support for the integration of key systems and applications with the Identity Management services, including KEANE, OACIS, Remedy, and APOC
- Tools and documentation to assist other legacy systems and applications with utilizing Identity Management services
- Provisioning of all directory-enabled accounts, principally the NetID. Other accounts will be considered on a case by case basis as they are integrated into the Enterprise Directory framework.

Identity and Access Management Service Charter

Solution Approach

As we proceed with implementing IdAM services, we will evaluate options with respect to commercial, open source, and/or in-house developed tools, always keeping in mind that “the primary purpose of the Identity and Access Management services is to supply information in standard formats and protocols so that systems and applications can utilize it to identify, authenticate and authorize users.”

1. Develop the broad schema for the physical Enterprise LDAP (following the “Identifiers, Authentication, and Directories: Best Practices for Higher Education”⁶ and “A Recipe for Configuring and Operating LDAP Directories”⁷).
2. Research requirements to sync Enterprise LDAP with Microsoft Active Directory and modify schema as necessary.
3. Implement minimum schema required to meet the immediate needs of the MNA and Microsoft Active Directory utilizing OpenLDAP and also be compliant with the standards established by the eduPerson task force⁸.
4. Clean up and match up the AD username space.
5. Institute new policies regarding username. The username will no longer be reassignable and it will be persistent.
6. Sync Microsoft Active Directory with the Enterprise LDAP. In the process of merging the MNA and AD accounts, users will register for the NetID. Registration will consist of choosing a username in compliance with the new policy established in Step 5. Since the existing MNA has stronger password security requirements than AD, the NetID registration process will also include choosing a password.
7. Integrate APOC with IdAM services
8. Decrease reliance on etc/password.
9. Continue rolling out the Person Registry application (perhaps renaming it).
10. Restructure the Person Registry relational database to follow best practices.
11. Integrate KEANE with IdAM services
12. Integrate OACIS with IdAM services
13. Rewrite webGAB as an Account Registry

Merging MNA and LYNX authentication has top priority, but steps 7 through 13 do not have to occur linearly. Integrating key applications will occur as soon as the opportune moment arises.

Assumptions

[HIPAA Security Policies](#) have already been devised to support and encourage use of the Identity and Access Management Service. “Whenever possible, MUSC Systems should authenticate their users through a centralized, standards-based authentication service. Proprietary, System-specific authentication procedures that require users to remember a separate password or access code, or to be issued separate access tokens, are strongly discouraged.” It is assumed that all systems needing to secure information will follow this policy. For each legacy system, the labor cost of integration will have to be weighed against the risk and continued labor expended managing identity and access in isolation. For each new system implemented, it assumed that it will utilize the Identity and Access Management Service, unless a compelling reason is given as to why not.

As systems are integrated with IdAM services, the security criteria regarding passwords or other access tokens will have to be evaluated to ensure that integration preserves the strongest security criteria.

Risks

If a flexible, robust, standards based Identity and Access Management Service is not provided, legacy systems will continue operating in isolation and new systems will build their own infrastructure from scratch. Privacy and Security regulations such as HIPAA will be increasingly difficult to meet. The longer it takes to deliver a sound Identity and Access Management Service, the greater the cost of retrofitting legacy systems.

⁶[Identifiers, Authentication, and Directories: Best Practices for Higher Education](#) Internet2 Middleware Initiative
May 9, 2000

⁷[A Recipe for Configuring and Operating LDAP Directories](#) Copyright © 2002 by Michael R Gettes, Georgetown
University, UCAID and/or the respective authors

⁸[eduPerson Object Class](#) web Copyright 1999-2005 EDUCAUSE

Identity and Access Management Service Charter

Conclusion

Once the Identity and Access Management Service is in place OCIO Information Services will be in a much better position to meet both the immediate needs of existing applications and the future needs of a broad range of “directory-enabled” applications and services .

Identity and Access Management Service Charter

Appendix A: Definitions

- **LDAP** - [The Lightweight Directory Access Protocol](#) (LDAP) was designed to remove some of the burden of X.500 access from directory clients, making the directory available to a wider variety of machines and applications. X.500, the Open Source Initiative (OSI) directory standard, defines a comprehensive directory service, including an information model, a namespace, a functional model, and an authentication framework. X.500 also defines the Directory Access Protocol (DAP) used by clients to access the directory.⁹
- **Kerberos** - “Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.”¹⁰
- **KEANE** - Keane Patcom Plus is MUSC'S Patient Registration and Accounts Receivable health care administration system.
- **OACIS** - Open Architecture Clinical Information System ([OACIS](#)) is MUSC'S Clinical Data Repository (CDR) system. As such it is a permanent residing place for patient information collected by ancillary services/departments, such as Lab, Radiology, Oncology, etc.
- **Remedy** – Remedy is the OCIO-Information Service's trouble call tracking system used by the [Support Desk](#).
- **AuthLDAP** - authldap.musc.edu is an OpenLDAP 2.1 server running SSLv2. Documentation is provided on how to authenticate against [AuthLDAP](#) on MUSC'S Web Server.
- **MUMPI** - MUSC Master People Index (MUMPI) is the relational database where identifying information from the MUSC'S core business systems of record is stored.
- **IDMS** – Sponsorship is part of the process of registering an Identity and storing it in MUMPI. The sponsorship of said Identity is stored and tracked in the IDMS (Identity Management System) relational database.
- **HERMIT** - Human Resources Management Information Technology (HeRMIT) is the Human Resource module of the GEAC Smartstream system utilized as MUSC's University Human Resource/Payroll system of record.
- **Colleague** – [Colleague](#) is the Office of Enrollment Services' system of record.
- **Sebastian** – Sebastian is the Human Resource module of the GEAC Smartstream system utilized as MUHA's Human Resource/Payroll system of record.
- **Person Registry Application** – [personRegistry](#) is the web application provided for registering and sponsoring a person's identity.
- **Phone Directory database** – The phone numbers published in the [Online Directory](#) website are entered by departmental "super users" via the [Phone Directory Administration Application](#) and stored in the MUSCphone_dir database.
- **GAB** – The Global Address Book (GAB) is used to administer the MNA, LYNX, Groupwise and OACIS account namespaces. [webGAB](#) is the administration tool.
- **myPOBox** - Campus PO Box numbers facilitate delivery of mail by the campus [Mail Service Center](#). The Mail Service Center establishes the valid campus POBox numbers. [myPOBox](#) is utilized associate a PO Box number with a person. PO Box numbers are published in the [Online Directory](#) website.
- **Entrabadge** - MUSC Badge system
- **Online Directory** website - The [Online Directory](#) has been in production since the last quarter of 2003. See [Currents](#) article. The Online Directory website utilizes the white pages LDAP.
- **IdmsREST** - Representational State Transfer (REST) is an architectural style for Web services. IdmsREST is web service providing Identity Management data.¹¹
- **Checkaccounts** – [Checkaccounts](#) is a web application provided for the purpose of checking the status of accounts (actually usernames) against IDMS and GAB.
- **IDMS Termination Notice** – Perl scripts have been written to allow System contacts (as registered in System Registry) to be notified when one of a user's Identity Sponsorships has terminated. At this time notification occurs via the medium of email.

⁹[The Lightweight Directory Access Protocol: X.500 Lite](#) Timothy A. Howes University of Michigan CITI Technical Report 95-8 27 July 27, 1995

¹⁰[Kerberos: The Network Authentication Protocol](#) copyright MIT April 12, 2005

¹¹[Building Web Services the REST Way](#) Roger L. Costello

Identity and Access Management Service Charter

- **MNA** - “A MUSC Network Account (MNA) is the key to online access for many applications on campus, both academic and clinical, as well as a login for [IMAP E-mail](#), [downloading software](#), [SunOne Calendar](#), [PPP](#), [Homerroom](#), [ftp](#), web accounts, and other accounts. This universal account is used for many "access required" web pages, as well as connecting to campus and applications from home. The users of these accounts must adhere to the [Computer Use Policy](#).” For further information refer to <http://www.musc.edu/infoservices/mna/index.html>.
- **System Registry** – System Registry is a web application which is utilized to register all MUSC computer systems and applications.
- **Etc/passwd** -
- **RADIUS** – Remote Authentication Dial In User Service (RADIUS is a protocol specified by the Internet Engineering Task Force (IETF) working group. There are two specifications that make up the RADIUS protocol suite: Authentication and Accounting. These specifications aim to centralize authentication, configuration, and accounting for dial-in services to an independent server.¹²
- **Microsoft Active Directory (AD)** – “Active Directory®, which is an essential component of the Windows 2000 architecture, presents organizations with a directory service designed for distributed computing environments. Active Directory allows organizations to centrally manage and share information on network resources and users while acting as the central authority for network security. In addition to providing comprehensive directory services to a Windows environment, Active Directory is designed to be a consolidation point for isolating, migrating, centrally managing, and reducing the number of directories that companies require.”¹³
- **Authenticator** – [Authenticator](#) is a MUSC Central Authorization tool.
- **IMAP email** - IMAP is the e-mail system for MUSC faculty, students and staff. It utilizes the Internet Message Access Protocol ([IMAP](#)).
- **SunONE Calendar** – [SunONE Calendar](#) is the calendar system for MUSC faculty, students and staff
- **HARPnet** – [HARPnet](#) stands for Homecare Agency Referral.
- **Dchart** – [Dchart](#) is the Incomplete Chart notification system.
- **LYNX** – [LYNX](#) is the Radia Software Distribution System
- **WebApps** – WebApps is a Citrix farm for clinical application accessibility.
- **VPN** – You can use the [VPN](#) client to gain access to resources normally restricted to MUSC network users like Homerroom file shares, standard IMAP e-mail (IMAPS is available without the use of VPN) and other traditionally insecure resources.
- **WebISO** – Web initial sign-on (WebISO). For more information see the [WebISO Working group](#).
- **Shibboleth** – [Shibboleth](#) provides a standards-based link between existing campus authentication systems and resource providers. It leverages campus identity and access management infrastructures to authenticate individuals and then sends information about them to the resource provider, enabling the resource provider to make an informed authorization decision.
- **PKI** – Public Key Infrastructure (PKI). For more information go to the [PKI Forum](#) and read “PKI Basics-A Technical Perspective.” And “PKI Basics - A Business Perspective”.
- **WebGAB** – [WebGAB](#) is the web application for the Global Address Book (GAB).
- **HIPAA** – MUSC is complying with the Health Insurance Portability and Accountability Act (HIPAA). For more information see the compliance web sites for the various entities: [MUSC University](#), [MUHA](#), and [UMA](#).
- **NMI-EDIT** - The primary goal of the NMI - Enterprise and Desktop Integration Technologies (EDIT) Consortium, part of the NSF Middleware Initiative (NMI), is to improve the productivity of academic scientists and higher education.

Appendix B: Systems Registered via System Registry

System	Description	Authentication Type
ACT CODED TESTING DATABASE	ACT Coded Testing Database	Active Directory (AD)
ACTIVE DIRECTORY DOMAIN	Active directory domain	Active Directory (AD)
ACT-TRACK	Software for hospital security	OS (Unix, Windows, etc.

¹² [RADIUS Authentication](#) Copyright © Ray Smith, 1996

¹³ [Active Directory](#) Copyright © Microsoft Corporation, 2005

Identity and Access Management Service Charter

AEROMED	Aeromed Helicopter Dispatch	PROPRIETARY
AGFA IMPAX	Picture Archive and Communication System	PROPRIETARY
AGFA WEB1000	Radiology Image Web Server	PROPRIETARY
ALUMNI EMAIL	Provides a resource for MUSC Alumni to create and maintain an e-mail address that forwards to an external e-mail account	MNA (Host DB)
AMANDA-I	Amanda backup server #1 - currently backing up about 35 servers on a nightly basis	MNA (Host DB)
AMANDA-II	Amanda backup server #2 - currently backing up about 5 servers on a nightly basis	MNA (Host DB)
AMOS.GI.MUSC.EDU	EUS Procedure Reporting Database	PROPRIETARY
ANSOS	Staff Scheduling	PROPRIETARY
APOLLO ADVANCE	Cardiovascular Information Management System	PROPRIETARY
ARC INTAKE	Intake office for Alcohol Research Center	NONE
ARCH	Bills for Cell phones	MNA
ARCP FINANCE	ARCP finance	PROPRIETARY
ARCP INTAKE PATIENT	Intake patient database	Active Directory (AD)
ARCP REGULATORY	ARCP Regulatory documentation	PROPRIETARY
ARCP SCHEDULING	ARCP Scheduling for patients	PROPRIETARY
ARCP STUDIES	ARCP Studies	Active Directory (AD)
ARGUS	Network traffic auditing	OS (Unix, Windows, etc.)
ASTRA CLASSROOM SCHEDULING	Classroom scheduling	PROPRIETARY
ATHENANET	Pt scheduling and registration data for Carolina Family Care	PROPRIETARY
AUDIX	Voice Mail	PROPRIETARY
AUTHGATEWAY	Firewall which enables access to MUSC network from public access points on LAN with MNA authentication	MNA (AuthLDAP)
AUTHORICATOR WEB	Web interface to AUTHORICATOR	MNA (AuthLDAP)
AUTHORIZATION FRAMEWORK	MUSC Central Authorization tool	MNA (AuthLDAP)
AXIUM	Complete Dental School Clinic Management Software	PROPRIETARY
BCR FILE STORE	File and program storage for Sybyl and Tripos programs used by BCR	MNA (Host DB)
BELL SOUTH	Bills for Bell South	MNA
BIG BROTHER	System Monitoring and Notification Server	MNA (AuthLDAP)
BIG IP	Load Balancing System	Active Directory (AD)
CALL MANAGEMENT SYSTEM	Call Management System for tracking call distribution	PROPRIETARY
CARDIOIMS	Departmental database housing reports, schedules, notes, etc for Pediatric Cardiology	PROPRIETARY
CARE MANAGER DATABASE	Tracking, Measuring, and Documenting activities of Care Managers for patients throughout the MUSC system	NONE
CATTS	Computerize Annual Training and Tracking System	LDAP (non-MNA)
CCIT KNOWLEDGE BASE	Knowledge Base	Active Directory (AD)
CELL BILLS	Cellular Bills on Web	MNA (AuthLDAP)
CENTRAMAX	Marketing Call Center	PROPRIETARY
CENTREX	Telephone Billing	PROPRIETARY
CENTREX WEB	View of Telephone Bills	PROPRIETARY
CERNER MSMEDS	Inpatient pharmacy information system	PROPRIETARY
CERNER PATHNET CLASSIC	Laboratory Information System	PROPRIETARY
CHECKGUARD	Check printing system for Payroll and Accounts Payable departments	PROPRIETARY

Identity and Access Management Service Charter

CINC	Current Insurance Claims	MNA
CISCO WORKS	Network management and configuration utility	PROPRIETARY
CITRIX WEBAPPS MUHA	Citrix Farm For Clinical Application Accessibility	Active Directory (AD)
CLINICAL OUTCOMES	Clinical outcomes for transplant	PROPRIETARY
CLINICMEMBERS.XLS	A listing of psychiatry outpatient clinicians	Active Directory (AD)
CLINITREND	clinical intervention documentation system for pharmacy	MNA
CLINLAN NDS TREE	ClinLAN NDS tree	PROPRIETARY
CME INTAGRAL	Attendance registry for department of Continued Medical Education	MNA (AuthLDAP)
CMN	Children`s Miracle Network	MNA
COAG	Patient info pulled from Cerner regarding Coag data	NONE
COLLEAGUE STUDENT SYSTEM	Student Information System	OS (Unix, Windows, etc.
COMMUNITY & PROFESSIONAL EDUCATION	The CPE database/reporting application is used by the Institute of Psychiatry (IOP) to track the professional development of medical staff.	NONE
COMPOUNDIT	Pharmacy Compounding Software	PROPRIETARY
CONSULTS	database that tracks patient records sent to/from MUSC for consultation	NONE
CONTRACT GRID.XLS	Listing of Psychiatry Managed Care Contracts	Active Directory (AD)
CROTHAL BED MANAGEMENT - TEAMCHIMES	Bed Management for House Keeping	OS (Unix, Windows, etc.
DARKWING_ACCESS	Access to the data warehous on the DARKWING database server	PROPRIETARY
D-CHART	Incomplete Chart notification system	MNA (AuthLDAP)
DENIALS2.MDB	Psychiatry Inpatient denials data base	NONE
DHCP	Dynamic Host Control Protocol	PROPRIETARY
DICTAPHONE	Radiology Voice dictation system	PROPRIETARY
DONOR DATABASE	Transplant Donor database	PROPRIETARY
DSPLUS	Pulmonary Rehab Spirometry Measurement System	Novell Directory Service (NDS)
EBADGE	Electronic Badge System	MNA (AuthLDAP)
ECHOVACS	View pediatric cardiac ultrasounds and reports	PROPRIETARY
EFFORT REPORTING	Tracks distribution of activities for employees as required by Federal OMB Circular A-21 and Medicare/Medicaid Cost Reporting	MNA (AuthLDAP)
EFFORT WEB	Effort Web Description	MNA (AuthLDAP)
EMAIL BACKUP	Emergency IMAP email system when main IMAP is down	MNA (Host DB)
EMAIL LDAP ADDRESSES	LDAP system containing email addresses	NONE
EMPLOYEE TRAINING REGISTRY	Risk Management`s database of employee training (OSHA, HIPAA, etc.)	MNA (AuthLDAP)
ENTRAPASS	Public Safety Card Access System	MNA
ENVIRONMENT OF CARE/INFECTION CONTROL AUDIT DB	Review of Environment of Care and Infection Control standards for regular review	NONE
EPEAR	ePEAR Address Change	MNA (AuthLDAP)
EPSI BUDGETING	MUHA Budgeting App	PROPRIETARY
ERAS	Resident Application Organizational Software	LDAP (non-MNA)
ESI NOVA	Central Supply Management	PROPRIETARY
EX-EKG DATABASE	storage of faxed ekg`s from external locations	MNA
EXTERNAL SMTP	Provides buffer for all externally originated e-mail destined for MUSC and provides SPAM filtering	MNA (Host DB)

Identity and Access Management Service Charter

FAC	Faculty Appointment Contract	MNA
FACULTY EFFORT REPORTING	Reimbursement Services Faculty Effort Reports (Medicare Funding)	PROPRIETARY
FILENET	Document Management System	PROPRIETARY
FINANCE NT DOMAIN	Finanace NT domain	LDAP (non-MNA)
FIREWALL REGISTRATION	Firewall Registration System	MNA (AuthLDAP)
FIREWALL RULES REQUEST / REGISTRATION	Web based firewall rules registration and request	MNA (AuthLDAP)
FLOCYTO	Patient info pulled from Cerner regarding flow cytometry data	NONE
FTE	Full Time Equivilant	MNA
GCA GRANTS MASTER	Grants & Contracts Accounting database application	OS (Unix, Windows, etc.
GCA_SPACE_STUDY	Determine indirect costs associated with grants	OS (Unix, Windows, etc.
GE VIEW POINT OB ULTRASOUND	OB ultrasound diagnostic diatbase	Active Directory (AD)
GEAC SMARTSTREAM FINANCIALS	University and Medical Center GL and financials application	PROPRIETARY
GEAC SMARTSTREAM HR - MUHA	Human Resource/Payroll Application for Hospital Authority	MNA
GEAC SMARTSTREAM HR - UNIVERSITY	Human Resource/Payroll System for University	MNA
GIS	Grants Information System	PROPRIETARY
GROUPWISE E-MAIL	GroupWise E-Mail	Novell Directory Service (NDS)
GTE	Bills for GTE	MNA
GYN SURGICAL DATABASE	Data from all gyn surgical procedure done by the member of MUSC OBGYN department	Active Directory (AD)
HARPNET	Homecare Agency Referral User Interface	MNA (AuthLDAP)
HEALTHSCRIBE	Dictation and Transcription System	PROPRIETARY
HEART.MDB	Access database for heart transplant program	MNA
HOMEROOM	Homeroom - Student and Faculty file store	MNA (Host DB)
HORIZON BUSINESS INSIGHT	McKesson - Report viewer / decision support	PROPRIETARY
HRDTS	Human Resources Document Tracking System	MNA
HTNWEB1.MUSC.EDU	Dr. Egan`s Hypertension Initiative Database	PROPRIETARY
IDX IMAGECAST	RADIOLOGY INFORMATION SYSTEM	PROPRIETARY
III	MUSC Library Catalog System (shared with USC School of Medicine)	NONE
IIS - MS INTERNET INFORMATION SERVICES	Microsoft Internet Information Services (Web Servers)	Active Directory (AD)
IMAGEQUEST	Reporting System that imports data and places images on Final Reports.	PROPRIETARY
IMAP	IMAP Mail system	MNA (Host DB)
IMAPS	External IMAP and IMSP secure tunnel for secure, external access to email	MNA (Host DB)
INFECTION CONTROL NOSOCOMIAL INFECTIONS DATABASE	Hospital Acquired Infections	LDAP (non-MNA)
INFOSPAN MC	Purchasing Card accounting for Medical Center	OS (Unix, Windows, etc.
INFOSPAN UNIVERSITY	Purchasing Card accounting for University	OS (Unix, Windows, etc.
INSTITUTE OF PSYCHIATRY -	Twice Monthly review of high alert medications for	NONE

Identity and Access Management Service Charter

HIGH ALERT MED DATABASE	documentation compliance	
INSTITUTE OF PSYCHIATRY - MAR DISCREPANCY DATABASE	Nursing and Pharmacy reporting and analysis of MAR discrepancies found	NONE
INSTITUTE OF PSYCHIATRY - NURSING INTENSITY	Measure intensity of Nursing Care given to patients in the Institute of Psychiatry	NONE
INTERNET FIREWALL	Internet firewall	OS (Unix, Windows, etc.
IWR-MEDICAL CENTER	Online Human Resource & Payroll Reports	PROPRIETARY
IWR-UNIVERSITY	Online Human Resource & Payroll Reports	PROPRIETARY
KEANE	Patient Registration and A/R	PROPRIETARY
KRONOS WORKFORCE TIMEKEEPER	Time and attendance	PROPRIETARY
KRONOS WORKFORCE WEB LABOR DISTRIBUTION	Time and attendance	PROPRIETARY
LABOR DISTRIBUTION	Processes salary distribution changes to create retroactive journal vouchers in payroll ledger and finance general ledger	MNA
LANVISION	Document Imaging System	PROPRIETARY
LIBRARY HEALTH WEB SERVER	Library Auxilliary Web Server, home to Hands on Health - SC, PICO, AHEC-IS, JUMP, Bioterrorism, and others	OS (Unix, Windows, etc.
LIBRARY WEB SITE	MUSC Library Primary Web Site	OS (Unix, Windows, etc.
MAGIC KINGDOM	Department of Pathology File Server	OS (Unix, Windows, etc.
MAIAL CLIENT BRAIN04	Sun Microsystems client for MAIAL	PROPRIETARY
MAIAL SERVER ATHENA	Sun Microsystems server for the Multidisciplined Advanced Image Analysis Lab (athena)	PROPRIETARY
MAIAL SERVER MINERVA	Dell 6650 Linux server for MAIAL (minerva)	LDAP (non-MNA)
MAIAL SERVER SOPHIA	Dell 650 Linux server for MAIAL (sophia)	PROPRIETARY
MAILHUB	Centralized email server designed to receive all email traffic that has to do with our area of responsibility. Also handles mailing lists	MNA (Host DB)
MAIN DNS SERVER	Main DNS server for MUSC	NONE
MAINTENANCE DATABASE	track all instruments and equipment in Pathology Labs and the maintenance of that equipment	NONE
MANAGER'S TOOLBOX	Hospital Management Reports	MNA
MAR DISCREPANCY DATABASE	Review/List of discrepancies found by nursing in the Medication Administration Record and Pharmacy follow-up	NONE
MAR HIGH ALERT DATABASE	bi-weekly review of high alert medication compliance	NONE
MCAFFEE FTP MUSC	FTP site for McAfee AntiVirus Updates	MNA
MCI	MUMPI Control Interface	MNA (AuthLDAP)
MCKESSON ACUDOSE/ROBOT	Automated medication cassette filling and automated dispensing cabinets	PROPRIETARY
MCKESSON -BAKER CELLS	Pill filling machine in Rutledge Tower pharmacy	NONE
MCKESSON ECONOLINK	Inventory module in pharmacy distribution center	PROPRIETARY
MDSTAFF	Resident and Physician Credentialing System	PROPRIETARY
MEDILINKS	Therapeutic Info System for Charting and Charge Capture	PROPRIETARY
MICROMEDEX	Provides comprehensive drug and toxicology information via a web interface	MNA
MICROSOFT WORD OFFICE (EXCEL AND WORD)	Spreadsheet and Word documents	Active Directory (AD)
MOHS_QA	Patient info pulled from Cerner regarding MOHS QA	NONE

Identity and Access Management Service Charter

	data	
MOM - MICROSOFT OPERATIONS MANAGER	Microsoft Operations Manager	Active Directory (AD)
MUHA HRDTS	Authority Human Resources Document Tracking System	MNA
MUMPI ADHOC	Ad Hoc Person Registry	MNA (AuthLDAP)
MUMPI ADHOC WEB	Ad Hoc person into MUMPI via the web	MNA (AuthLDAP)
MUSC DEVELOPMENT WEBSERVER (PRIMARY)	Development server for the primary corporate/university webserver.	MNA (Host DB)
MUSC WEBSERVER (PRIMARY)	University/Corporate MUSC webserver, Roaming preference server.	MNA (Host DB)
MUSC_FINANCIAL_REPORTS	Monthly Financial reports	OS (Unix, Windows, etc.)
MUSCHEALTH.COM	MUSC public website	NONE
MUSE EKG SYSTEM	EKG Acquisition and Archive system	PROPRIETARY
MYPROVOST	Reporting tool for Provost Database	MNA (AuthLDAP)
NETSCOUT	Network Baseline and trending	PROPRIETARY
NUCMED	Nuclear Pharmacy Program	NONE
NUCMED PHARMACY	Dupont Nuclear Medicine Pharmacy Info Sys	PROPRIETARY
NURSING INTENSITY DATABASE	Measures intensity of nursing care provided to patients	NONE
OACIS	Clinical data repository, results review & census management	PROPRIETARY
ORTHOPAEDIC SURGERY INQUIRY	excel spreadsheet	Active Directory (AD)
OVID	MUSC Article Indexes used by MUSC faculty, staff and students	MNA (Host DB with customizations)
OZ	provide dial in remote access	MNA
OZ2	dial in for remote users	MNA
PACE	Personal Assessment of Course Effectiveness	MNA
PAIGE	E/D Patient Discharge Instructions	NONE
PANELS AND RATES	Contracted insurance panels and rates for psychiatry. Folder also holds worksheets with PHI in them.	NONE
PARKIT	Parking Information Technology	MNA (AuthLDAP)
PARKIT RENEWAL	Parking Information Technology Parking Renewal on Web	MNA (AuthLDAP)
PARKIT WAITING LIST	Parking Information Technology Waiting List on Web	MNA (AuthLDAP)
PATHWEB	Pathology Department Web Server	OS (Unix, Windows, etc.)
PEDIATRIC RESIDENTS ELECTRONIC CHECKOUT SHEETS	Electronic checkout sheets for peds residents	MNA
PEDS CARDIOLOGY BIG BROTHER	big brother server for pediatric cardiology	NONE
PEDSLINUX	Pediatrics File Server	SAMBA (Unix Share)
PEOPLE ADMIN - MEDICAL CENTER	Web based (ASP Model) Applicant Tracking System - University	PROPRIETARY
PEOPLE ADMIN - UNIVERSITY	Online Applicant Tracking System	PROPRIETARY
PERSONAL WEBSITE SERVER	Serves public_html directories.	MNA (Host DB)
PHARMACY EMBOSsing	Ability to insert, modify and delete physician information used for prescription cards. Also sends data to printer to create a prescription card.	MNA (AuthLDAP)
PHYSICAL PLANT WORK	Work Order System	PROPRIETARY

Identity and Access Management Service Charter

ORDER SYSTEM		
PI_KEY	Tacking Principal Investigator/UDAK Project assignment	PROPRIETARY
PIF	database that tracks specimens sent to outside labs	NONE
POSEIDON	E/D Triage	NONE
PRACTICE PARTNER	Ambulatory Care Electronic Medical Record	PROPRIETARY
PRIMUS	Professional Information for Musc	MNA
PROLINC	Professional Liability Insurance Claims	MNA
PROVOST	Faculty appointments and promotions as entered by data administrators	MNA (AuthLDAP)
PROVOST TERMINATION NOTICATION PROCESS	Psuedo system entered in order to notify Provost of Faculty Terminations	PROPRIETARY
PROWL	Professional with Liability	MNA (AuthLDAP)
PROWL WEB	Professional with Liability for Web	MNA (AuthLDAP)
PYXIS - MUSC BADGE INTERFACE	Interface between MUSC Badge system and Pyxis Supply System	PROPRIETARY
PYXIS SUPPLY MANAGEMENT	Supply Management and Dispensing	PROPRIETARY
QMI-LABOR AND DELIVERY	Fetal Monitoring with Archive	PROPRIETARY
QS1	Outpatient pharmacy application	PROPRIETARY
QUALITY COUNCIL	Confidential MUHA Quality Council Information	MNA
RADIA	Radia Software Distribution System	Active Directory (AD)
RADIATION SAFETY DATABASE	Safety data accumulation / investigators info/ charges	OS (Unix, Windows, etc.
RADIUS	authentication server	MNA (Host DB)
READMISSION AND BOUNCEBACK DATABASE	Tracking/Reporting database for all MUSC Readmissions and ICU bouncebacks	NONE
REMEDY	CCIT trouble call tracking system	PROPRIETARY
RENALSTAR	Dialysis Info System	PROPRIETARY
RFCOORDFMP	Referral information for the Inst of Psychiatry	NONE
RIOGRANDE.MUSC.EDU	Web Protocols	MNA
ROOT NDS TREE	Netware NDS ROOT tree	PROPRIETARY
SAMBA HR STORAGE REPOSITORY	Samba Storage Repository for HR Users	NONE
SARCDATAB	clinical data corning sarcoidosis patients	NONE
SIMON CALL CALENDARS	Administration of ONLINE CALL SCHEDULES	PROPRIETARY
SIMON PAGING	Campus Paging System	NONE
SITE EXECUTIVE (WWW.MUSCHEALTH.COM)	Web Content Management System (CMS)	MNA (AuthLDAP)
SMTP	Internal email buffer responsible for the relaying of unauthenticated, internally generated correspondence	MNA (Host DB)
SMTPS	External email buffer responsible for the relaying of authenticated, internally generated correspondence	MNA (Host DB)
SOCIAL WORKER DATABASE	Database to Monitor, Track, and Document for patients being followed by Social Workers	NONE
SOLIMAR PRINT/DIRECTOR	Print/Director for Xerox DP 115MX printers - PDF file creator and indexer	PROPRIETARY
SPECIMEN COLLECTION HANDBOOK	database used to update Pathology Lab Test data	PROPRIETARY
STERILE PROCESSING MICROSYSTEMS	Sterile equipment tracking system	PROPRIETARY
STUHOUSE	Listing of off campus housing	MNA (AuthLDAP)
SURGISERVE	OR Scheduling	PROPRIETARY
SYNCHRONIZE	Classroom Scheduler	MNA
SYSTEM REGISTRY	Registry of all MUSC computer systems and	MNA (AuthLDAP)

Identity and Access Management Service Charter

	applications	
TACACS	TACACS	MNA
TOOL FOR IMPLEMENTING AGENCY NURSING INFORMATION	The TITANIC database/reporting application is used by Clinical Services Administration to manage medical staff positions for the hospital which are held by outside agency medical personnel.	NONE
TRANSCRIPTION LOG DATABASE	Outsource Transcription Log Database	Novell Directory Service (NDS)
TRAUMA REGISTRY	Trauma outcomes mgmt/reporting	PROPRIETARY
TRENDSTAR	Financial forecasting software and database	OS (Unix, Windows, etc.
TXPCP	Transplant patient care database	PROPRIETARY
UMA/CFC DOMINO SERVER	Domino Server	PROPRIETARY
UMA/CFC EMPLOYEE SELF SERVICE	Employee/Payroll/Benefit Self Service	PROPRIETARY
UMA/CFC INFINIUM HR/PY	Payroll & Human Resources	PROPRIETARY
UMA/CFC INFINIUM GENERAL LEDGER & REPORT WRITER	General Ledger / Report Writer	PROPRIETARY
UMA/CFC INFINIUM PAYABLES LEDGER/ACCOUNTS PAYABLE	Payables Ledger / Accounts Payable / Income Reporting	PROPRIETARY
UMA/CFC KRONOS	Kronos TKAS	PROPRIETARY
UMA/CFC NORTHBRIDGE NT SERVER	Windows 2000	PROPRIETARY
UMA/CFC RFILEMANAGER @ NORTHBRIDGE	RFileManager	PROPRIETARY
UMA/CFC RFILEMANAGER @ PARKSHORE	RFileManager	PROPRIETARY
UMA/CFC SPYVIEW	Spyview by Magellan	PROPRIETARY
UMAREQUESTS_CURRENT.M DB	Data base of UMA requests for information	Active Directory (AD)
UMS	Web base financial management system	PROPRIETARY
UNICOMM	University Communications` web site	NONE
UPS - EXIDE IN 3CH	UPS for 3CH computer room	NONE
VENDOR BILLING INTERFACE SYSTEM	Application for processing electronic billing interfaces to SmartStream Financials	OS (Unix, Windows, etc.
VERITAS NETBACKUP - CLINICAL SYSTEMS	Centralized Clinical System Backup/Restore	OS (Unix, Windows, etc.
VIEWDIRECT	Report distribution server for Keane financial reports	PROPRIETARY
VIVID 7	Cardiology EchoCardiogram System	PROPRIETARY
VMAX	Pulmonary Function Testing	PROPRIETARY
VPN1.CCIT.MUSC.EDU	Cisco VPN 3030 Concentrator	MNA (Host DB)
WEBADVISOR	Colleague Web interface for grades, tuition payments, etc	MNA (AuthLDAP)
WEBCT 3.8CE	Used by faculty to develop & deliver online, web-based course materials & examinations	MNA (Host DB)
WEBGAB	Administor MNA, Groupwise and Ocis account Namespaces	MNA (AuthLDAP)
WEBMAIL.MUSC.EDU	Web client for IMAP e-mail	MNA (Host DB)
WINDOWS UPDATE / SUS	Windows Update Service	MNA
WWW2.MUSC.EDU	Academic WEB server	OS (Unix, Windows, etc.
XEROX	Bills for Xerox	MNA

Identity and Access Management Service Charter