A Report for

National Institutes of Health

Collaboration Architecture

18 July 2003
Engagement: 220441441

research consulting measurement community news

Gartner

Table of Contents

List of Figures

List of Tables

1.0 Introduction

Collaboration is vital in achieving the NIH mission. This report establishes standards and guidelines to apply across NIH, while forging a common vision of the future for enterprise messaging at NIH.

1.1 Collaboration Domain Team

This report comprises the compilation of findings and recommendations derived from the joint NIH-Gartner Enterprise Architecture project team. A team of nine subject matter experts from various Institutes and Centers (ICs) and Center for Information Technology (CIT) worked together for 12 weeks to develop the Collaboration architecture patterns and bricks that are presented in this report. The following ICs and their representatives contributed to this effort:

- Rajesh Bhandari, NLM
- Tom Carrington, NCI
- John Deermer, OD
- Kevin Hobson, CIT
- Kim Kassing, NIAID
- Todd Myrick, CIT
- Scot Ryder, NIDCD
- Chris Stenger, OD
- Valerie Wampler, CIT

1.2 Scope

The context of the NIH Collaboration Domain Project is NIH's Messaging and Directory systems, with the Collaboration Domain Team concentrating upon the Enterprise e-Mail System and Enterprise Directory. Directives from the Department of Health and Human Services (DHHS) provided further detail to the e-mail environment, requiring a consolidated system for all of NIH, resulting in the standardization upon Exchange 2000 for e-mail services and Active Directory networking services.

The concentrated scope, Table 1, allowed the Collaboration Domain Team to analyze, collaborate and develop consensus in a timely and efficient manner. The Collaboration Domain Team did not exhaustively cover every aspect of the Collaboration & Information Delivery and Directory Services domains, but instead focused upon the enterprise messaging and Network Operating System (NOS) services.

Table 1. Data & Information Technology Taxonomy Map

Domain	Sub-Domain	Element ■ Sub-Element
Collaboration and Information Delivery		
	Collaboration	
		Calendaring and Scheduling
		Messaging ❑ e-Mail ❑ Instant Messaging
		■ Other
Directory Services		
	Enterprise Directories	

1.3 NIH Architectural Matrix

The Collaboration Domain Team used the NIH Architectural Matrix as an organizing framework for our analysis, see Table 2.

Table 2. Enterprise Messaging NIH Architectural Matrix

	Data Architecture	Application Architecture	Technology Architecture
Planner View	❑ **Data Architecture from the Planner View (Section 1.3.1).** High-level business objects which are the enterprise messaging system.	N/A	❑ **Technical Architecture from the Planner View** (Section 1.3.3).
Owner View	❑ **Data Architecture from the Owner View (Section 1.3.2).** High level semantic model for the business objects uncovered by the Planner View.	N/A	❑ **Technical Architecture from the Owner View** (Section 1.3.4).
Designer View	N/A	❑ **Logical Design Pattern of the consolidated Messaging System (**Section 2.0).	❑ ► **Technical Architecture from the Design View** (See Networking Architecture)
Builder View	N/A	❑ **Draft Physical Design Pattern of the consolidated Messaging System** (Appendix D).	❑ **Bricks** (Section 3.0).
Subcontractor View	N/A	N/A	

Data Architecture from the Planner View

The Collaboration Domain Team came to a consensus on the business objects of NIH's enterprise messaging system. Each object is mapped to its Data Architecture equivalent (► see Data Architecture Domain Report).

- Party [Party]
- Messages [Assets]
- Calendar [Events]
- Contacts [Party]
- Resources [Assets]
- Collaborative Objects [combination of Party, Location, Assets and Events][1].

[1] The number of different Data Classes used in describing Collaborative Objects is an indication of relationships between the Data Classes.

Data Architecture from the Owner View

The Collaboration Domain Team further decomposed the business objects of NIH's enterprise messaging system into a high-level semantic model.

- **Party**—Organizations, Groups[2], Persons
- **Messages**—Mail (Embedded, Multi-Media), Attachment
- **Calendar**—Appointment, Task, Resource Schedule
- **Contacts**—Address books, Distribution Lists
- **Resources**—Equipment, Conference Room
- **Collaborative Objects**—Documents, Work Flow.

Technical Architecture from the Owner View

NIH's business locations and partners span the globe, as such NIH has research fellows and facilities distributed in many different countries performing functions that are core to NIH's mission and vision.

- Global.

Technical Architecture from the Owner View

Email messages and attachments allow NIH to support asynchronous written communication among individuals without mediation.

- NIH Network
- Public Internet.

1.4 Principles

Through a number of consensus building workshop exercises, the Collaboration Domain Team developed the principles shown in Table 3. The principles are intended to embody the spirit of the Collaboration Domain effort at NIH.

[2] Groups are a collection of Parties (Persons) who share a common attribute.

Table 3. Principles Developed by the Collaboration Domain Team

Principles	Rationale
Principle #1: Security is fundamental to Collaboration Systems and shall be based upon the sensitivity of data generated and maintained, meeting or exceeding the directives of departments or agencies with oversight.	With the introduction of stricter government mandates, such as HIPAA, and the increasing digitization of sensitive information, any Collaboration System must be grounded in an appropriate level of security, balancing the sensitivity of the data with ease of use.
Principle #2: Collaboration Systems shall leverage existing and future enterprise software, management systems, infrastructure and standards.	As a practical matter, NIH has invested heavily in a number of technologies, infrastructures and standards; therefore any system hoping to enjoy wide use will need to leverage as much investment as possible.
Principle #3: Collaboration Systems shall integrate with enterprise Application and Directory structures and support the import and export of information, facilitating sharing at NIH.	Any system used will need to interface with the appropriate existing systems at NIH.
Principle #4: Collaboration Systems shall provide common access for authorized personnel and offer full access from all supported platforms. Common access for authorized personnel includes: ❑ Access from supported platforms and user interfaces ❑ Access within NIH ❑ Access via secure remote connectivity.	Because of NIH's global character, any successful enterprise collaboration system must address the requirements of NIH's user communities, especially in regard to remote access, access within NIH and platform support.
Principle #5: Collaborative Systems shall be based upon industry best practices and open standards.	In order to effectively manage risk, NIH requires that any collaboration system employed be based upon open standards, when possible, and best practices.

The principles were used in guiding the Collaboration Domain Team through the decision making process of developing the future-state architectures for e-mail and Active Directory (AD) at NIH. By referring back to the principles, the Collaboration Domain Team ensured that the outputs from the various architectural exercises were consistently aligned and that decisions were internally congruent with one another.

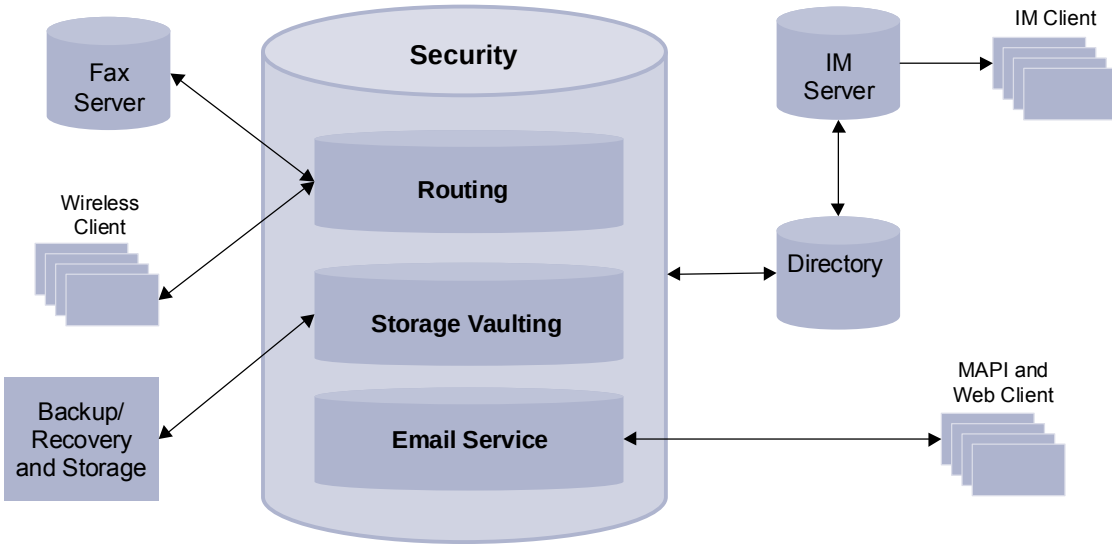
2.0 Enterprise Messaging Pattern

2.1 Messaging Pattern

Description and Context

The Enterprise Messaging Pattern is of a future-state of a single consolidated NIH-wide e-mail system, Central e-Mail Services (CES), which combines the various messaging systems into one logical system, Exchange 2000, shown in Figure 1. All inbound/outbound messaging traffic will be monitored, maintained and administered from a central location.

Figure 1. Future Logical State of the Enterprise Messaging System



Collaboration Domain Team Meeting 17 – 13 May 2003

The logical representation is independent of the physical architecture employed. The physical architecture is outlined by the enterprise messaging bricks, section 1.7. CIT provided a technical draft physical state, see Appendix D.

Business and IT Drivers

- DHHS directive to consolidate e-mail services
- Cost and complexity reduction
- Universal set of collaborative tools (e.g., Calendaring, Directory, Shared Folders, etc.).

Solution

Centralizes the Routing, e-Mail Services and Storage of electronic communications and attachments.

- Provides a single e-mail messaging system
- Provides for a consistent and scalable messaging solution for the entire enterprise.

Benefits (Goals)

- Allows for 24x7 customer service and hardware support
- Allows for the timely updating of the e-mail system
- Supports the implementation of best practices
- Provides defined service-level agreements (SLAs)
- Reduces overall costs, while providing a minimum guarantee of operability to all ICs
- Provides a standard product suite with Collaboration benefits and reduced training expenses.

Limitations

- May reduce the flexibility and responsiveness of some member ICs
- May disrupt informal support networks.

Assumptions

- All new accounts will be created in the NIH AD
- Exchange will be the standard e-mail service for all NIH users
- The AD framework will be used to manage the Exchange service
- All non-Exchange “administrative” e-mail systems will be migrated to Exchange by 1 October 2003, and legacy e-mail systems will be retired to realize the cost savings.

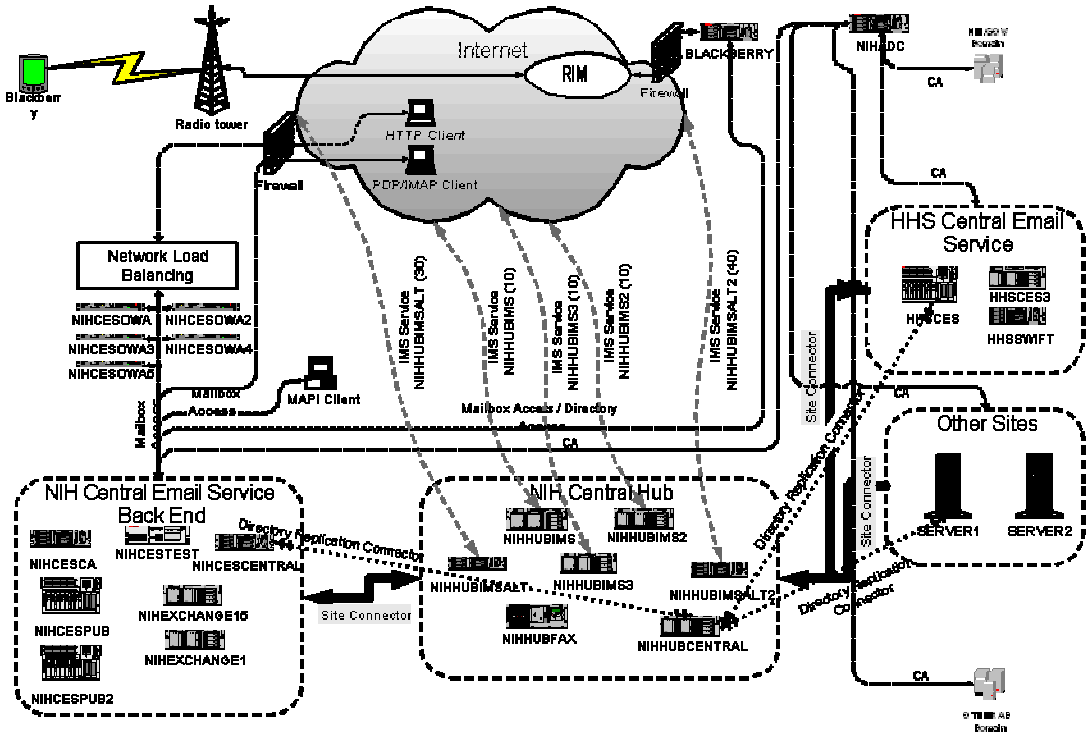
2.2 Exchange 5.5 e-mail Current State

The Collaboration Team analyzed the federated structure of the current enterprise e-mail environment at NIH. This analysis was supplemented by the measurement study that was simultaneously conducted by a separate NIH team and Gartner. During week 5 of the Collaboration Domain Team’s efforts, a directive was made from DHHS to NIH to consolidate its various enterprise e-mail systems into a single product and implementation. NIH selected Exchange and is currently implementing this product. Therefore, much of the logical current state information gathered by the Collaboration

Domain Team, Figure 1 above, is undergoing change. In order to accommodate the dynamic nature of the environment, the Collaboration Team, in consensus, constructed a logical representation of the future state, see Figure 3.

The current state CIT Exchange e-mail System, see Figure 2, serves approximately 80 percent of NIH email accounts. The physical architecture uses a centralized hub consisting of load balanced in and out bound queues (Central Hub in Figure 2). IC systems are hosted on centrally managed servers (NIH Central Email Service Back End in Figure 2), with some small IC's sharing physical servers. NIH also hosts the HHS Central Email Service, which is physically and logically separate from the existing NIH network at the operational level. All servers are backed-up through a centralized archival system maintained by CIT.

Figure 2. CIT Exchange e-mail System, Current State



Source: CIT

As a result of the DHHS directive the current state is undergoing a considerable amount of change, currently making it difficult to capture a traditional "current state" snapshot. To better understand the current composition of the enterprise e-mail architecture, the expected migration diagram, produced by CIT, has been included in this document, see Figure 3. The migration plan depicts the expected migration path of all NIH enterprise e-mail accounts.

Solution

Centralizes the Routing, e-Mail Services and Storage of electronic communications and attachments.

- Provides a single e-mail messaging system
- Provides for a consistent and scalable messaging solution for the entire enterprise.

Benefits (Goals)

- Allows for 24x7 customer service and hardware support
- Allows for the timely updating of the e-mail system
- Supports the implementation of best practices
- Provides defined service-level agreements (SLAs)
- Reduces overall costs, while providing a minimum guarantee of operability to all ICs
- Provides a standard product suite with Collaboration benefits and reduced training expenses.

Limitations

- May reduce the flexibility and responsiveness of some member ICs
- May disrupt informal support networks.

Assumptions

- All new accounts will be created in the NIH AD
- Exchange will be the standard e-mail service for all NIH users
- The AD framework will be used to manage the Exchange service
- All non-Exchange “administrative” e-mail systems will be migrated to Exchange by 1 October 2003, and legacy e-mail systems will be retired to realize the cost savings.

2.2 Exchange 5.5 e-mail Current State

The Collaboration Team analyzed the federated structure of the current enterprise e-mail environment at NIH. This analysis was supplemented by the measurement study that was simultaneously conducted by a separate NIH team and Gartner. During week 5 of the Collaboration Domain Team’s efforts, a directive was made from DHHS to NIH to consolidate its various enterprise e-mail systems into a single product and implementation. NIH selected Exchange and is currently implementing this product. Therefore, much of the logical current state information gathered by the Collaboration

3.0 Enterprise Messaging Bricks

The Collaboration Domain Team has developed five bricks each detailing a separate segment of the enterprise messaging system: Messaging Systems, Protocols, Server OSs, Client OSs and Collaboration Clients.

Each brick is used to better describe the consolidated collaboration patterns. To provide improved fidelity in the mainstream brick category, the category was divided into Tactical (0-2 years) and Strategic (2-5 years) time frames. ► The Brick concept is further explained in the Architecture Introduction.

3.1 Messaging Servers

Enterprise messaging systems currently in use at NIH:

Table 4. Messaging Servers Brick

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ Exchange 5.5 ■ Instant Messaging (various technologies) ■ Blackberry ■ GroupWise (NLM) ■ Send Mail (SMTP/relay) ■ Helix ■ CODON ■ KRONOS ■ Fax ■ Netscape Messaging Server ■ Meeting Maker ■ Wylbur	■ Exchange 2000 ■ Blackberry (RIM Server) ■ Instant Messaging (various technologies) ■ Listserv	■ Exchange 2003 ■ Additional Wireless (Palm, etc.)
Retirement Targets (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
■ Netscape Messaging Server ■ Meeting Maker ■ Wylbur	■ Exchange 5.5 ■ GroupWise (NLM) ■ Send Mail (SMTP/relay) ■ Helix ■ CODON ■ KRONOS ■ Fax	■ Unified Messaging

Comments
■ For a successful Exchange 2000 migration, Active Directory (AD) must be in place. To gain the largest benefits from the Exchange 2000 system (more databases per server), AD must be running in its native mode. ■ Mac OS X MAPI Client not yet released (Q4—2003) preventing the widespread use of the new Exchange infrastructure by NIH's considerable Mac population. 11 June 2003

3.2 Protocols

Protocols in use by the enterprise messaging systems at NIH:

Table 5. Protocols

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ LDAP ■ SMTP ■ MAPI ■ IMAP ■ HTTPS ■ POP ■ HTTP	■ LDAP ■ SMTP ■ MAPI ■ IMAP ■ HTTPS	■ S/MIME
Retirement Targets (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
■ None	■ POP ■ HTTP	■ SOAP
Comments		
■ NIH is aggressively implementing security protocols in order to provide a more secure messaging environment, resulting in the introduction of many "secure" protocols. 11 June 2003		

3.3 Server OSs

Server OSs in use by the enterprise messaging systems:

Table 6. Server OSs

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ Win2000 ■ UNIX ■ NT 4.0 ■ Solaris	■ Win2000 ■ UNIX	■ Win2003

Retirement Targets (Technology to eliminate)	Containment (No new deployments)	Emerging (Technology to track)
■ NT 4.0 (monitoring system)	■ Solaris (NCI, only mail)	■ Linux
Comments		
■ NIH will be standardizing the back office servers during the consolidation process. 11 June 2003		

3.4 Client OSs

Client OSs in use by the enterprise messaging systems:

Table 7. Client OSs

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ WinXP ■ Win9X ■ Linux ■ UNIX ■ Mac OS 8, 9, X	■ Mac OS X ■ WinXP ■ UNIX	
Retirement Targets (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
■ Win9X ■ Mac OS 8 or earlier	■ Mac OS 9	■ Linux
Comments		
■ Increasing support costs are directly related to the amount of software diversity supported. 11 June 2003		

3.5 Clients Software

Client software used to access the enterprise messaging systems:

Table 8. Clients Software (Front-End)

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ Eudora ■ Outlook ■ Entourage ■ Outlook Web Access ■ UNIX/Linux (Pine, Elm, etc.) ■ Fetch Mail (POP Client) ■ Exchange Client ■ Meeting Maker ■ GroupWise (NLM)	■ Outlook ■ Pine (UNIX/Linux) ■ Elm (UNIX/Linux) ■ Eudora	■ Entourage ■ Outlook Web Access ■ Web Browser ■ High-End Calendaring Add-Ins

■ Wylbur		
Retirement Targets (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
■ Exchange Client ■ Meeting Maker ■ GroupWise (NLM) ■ Wylbur	■ Fetch Mail (POP Client)	■ OS X Mail
Comments		
■ NIH has a diverse client software base. This diversity results in additional maintenance and upkeep expenses. Unless the variation in clients serves a real business need, Gartner recommends that official support be limited to two or three client software packages. 11 June 2003		

4.0 Active Directory NIH Architecture Matrix

The Collaboration Domain Team used the organizing framework of NIH's Architecture Matrix to examine the Active Directory implementation at NIH.

Table 9. Enterprise Active Directory NIH Architectural Matrix

	Data Architecture	Application Architecture	Technology Architecture
Planner View	N/A	N/A	N/A
Owner View	N/A	N/A	❑ **Technology Architecture from the Owner View** (Section 4.2, partial).
Designer View	N/A	❑ **Logical Design Pattern of the enterprise NOS** (Section 4.3).	N/A
Builder View	N/A	N/A	❑ **Bricks** (Section 5.0).
Subcontractor View	❑ **Data Architecture from the Subcontractor View** (Section 4.1).	N/A	

4.1 Active Directory Data Standards

Active Directory is the physical representation of the Enterprise Directory, providing business policies and processes with technical resources built upon identity and network access.[3] The Collaboration Domain Team recognized the need for data standardization within the enterprise directory to facilitate the seamless exchange of data. Currently, many barriers exist to this free flow of data, as expressed to the Domain Team through an internal directory presentation.[4]

Data from the meeting exposed inconsistencies within data fields populated by each IC, and duplication of user account names. An example of the data field inconsistencies is captured in Table 10 below.

[3] Collaboration Domain Team Meeting 12, 25 April 2003.
[4] Keith Gorlen of CIT, Collaboration Domain Team Meeting 11, 22 April 2003.

Table 10. Data Field Population Counts

DOMAIN	TOTAL	DEPARTMENT	DESCRIPTION	DISPLAYNAME	EMPLOYEEID	GIVENNAME	INFO	MAIL	MIDDLENAME	PERSONALTITLE	PHYSICALDELIVEROFFICENAME_BG	PHYSICALDELIVEROFFICENAME_ORG	POSTALCODE	SECRETARY	SN	STREETADDRESS	TITLE
NIH	5,019	4,943	4,018	5,013	36	4,748	3,252	4,988			31	3,290	1,307	2,171	4,741	3,631	953
NCI	4,966	1	1,754	4,945	4,966	4,963		3,898			1,009	50	2		4,966	2	4,429
CC	2,788	2,680	2,726	2,787	132	2,650	53	2,680			2,595	16	2,676	3	2,643	2,680	101
NIAID	2,724	2,571	2,578	2,724	156	2,712	534	2,587	1		484	1,738	880	75	2,701	2,463	553
ORS	2,076	2,061	1,991	2,076	98	1,997	1,939	2,064			145	1,853	281	1,158	2,017	1,804	139
OD	1,647	1,625	1,628	1,647	155	1,608	69	1,557				1,606	1,534	1,540	1,616	1,610	57
NHLBI	1,611	1,588	1,611	1,611	1	1,573	932	1,611	3			1,594	200	212	1,586	1,534	592
NIEHS	1,507	1	1,501	1,507	1,507	83	1	4			1		1		83	1	1
NICHD	1,420	1,321	1,395	1,420	1,012	1,416	1,224	1,320			1	798	100	771	1,416	1,207	92
NINDS	1,067	1,043	978	1,067		1,064	94	1,067			21	997	12	10	1,059	1,021	665
NLM	809	46	796	809	809	782		677			316	260	23		784	53	179
NIA	770	737	768	770	631	769	160	745			407	252	312	166	770	384	45
NIMH_IRP_OD	684	671	246	684	392	633	34	611			2	593	593	421	639	580	498
NIDAIRPDOM	534	530	50	534		533	3	534			33	123	534		522	534	9
NIAMS	419	416	415	419	293	406	350	419			3	410	75	134	406	397	62
NEI	414	405	357	414	99	404	9	408			2	400	403	378	402	402	3
NIDCD	288	231	195	288	102	282	190	232	4		41	141	60	95	282	222	12
TOTAL	28,743	20,870	23,007	28,715	10,389	26,623	8,844	25,402	8	0	5,091	14,121	8,993	7,134	26,633	18,525	8,390

Source: Keith Gorlen of CIT, Collaboration Domain Team Meeting 11, 22 April 2003.

In order to address these inconsistencies, the Collaboration Domain Team has developed standards for the mandatory fields captured by the Active Directory from a collaboration domain perspective. This standards document is included as Appendix B within this report.

4.2 Active Directory Suppliers and Consumers

The Collaboration Team conducted surveys, included in Appendix C, which identified the suppliers and consumers of Active Directory services. The importance of capturing supplier and consumer information is to ensure that important Active Directory services—those used by ICs—are maintained and properly managed against risk, while unused services can be pared back or removed. A high-level supplier and consumer analysis (see Table 11, Surveys are included in Appendix C) provides a snapshot of who is using which Active Directory service at NIH and how these services are being used. Table 11 lists first the IC and then the technology used to supply/consume the service.[5]

Table 11 is organized in three columns: Service – the directory service used, Supplier – An entity (person, application, organization) which provides a service (information, authentication, etc.) to a Consumer, and Consumer – An entity (person, application, organization, etc.) which uses a service (information, authentication, etc.) of a Supplier. The rows in Table 11 refer to the Active Directory services used within each IC. The rows were developed by consensus of the Collaboration Domain Team.

[5] All ICs were surveyed and the following responded in time to be analyzed within this report (CC, NCCAM, NCI, NEI, NHGRI, NIAAA, NIAMS, NIBIB, NIDA (IRP & NSC), NIDDK, NIMH and OD). All surveys are attached in Appendix B.

Table 11. Active Directory Suppliers & Consumers

Service	Supplier	Consumer
Application Login	■ NIDA(NSC) – NIDA	■ NIDA(NSC) – NIDA
Application Authorization	■ NINDS – NINDS (Technology unknown) ■ NHLBI – eDirectory ■ NIDA(NSC) – NIDA (Technology unknown)	■ NINDS – NINDS (Technology unknown) ■ NIDA/IRP – Clinical Data Warehouse (CDW), RPA (i.e., Request for Purchase Action) ■ NHLBI – NHLBI (Technology unknown) ■ NIDA(NSC) – NIDA (Technology unknown)
Synchronization - Password	■ NINDS – MS Services for Unix, Authentix ■ NHLBI – eDirectory ■ NIDA(NSC) – provided by CIT ■ NIMH – AD ■ NCI, NCCAM & NIBIB – DirXML	■ NINDS – NINDS (Technology unknown) ■ NHLBI – AD ■ NIDA(NSC) – NIDA (Technology unknown) ■ NIMH – AD ■ NCI, NCCAM & NIBIB – DirXML, NCI, NCCAM & NIBIB
Synchronization - Directory	■ OD – OD (Technology unknown) ■ NINDS – Receipt and Referral, FinEx, Remedy, Outlook, Terminal Server, Remote Access App, Person Org. Manager ■ NHLBI – eDirectory ■ NIDA(NSC) – provided by CIT ■ NCI, NCCAM & NIBIB – eDirectory	■ OD – OD (Technology unknown) ■ NINDS – NINDS (Technology unknown) ■ NHLBI – AD, Exchange, Linux ■ NIDA(NSC) – NIDA (Technology unknown) ■ NCI, NCCAM & NIBIB – eDirectory
DNS	■ CC – DDNS, provided by CIT ■ NIDA(NSC) – provided by CIT ■ NIMH – provided by CIT/BOSB ■ NCI, NCCAM & NIBIB – provided by CIT/BOSB ■ NEI – provided by CIT	■ CC – CC (Technology unknown) ■ NIDA(NSC) – NIDA (Technology unknown) ■ NIMH – NIMH (Technology unknown) ■ NCI, NCCAM & NIBIB – Users ■ NEI – NEI Clients
Policies	■ OD – Admins ■ NHLBI – eDirectory ■ NIDA(NSC) – provided by CIT ■ NEI – NEI Domain Controllers	■ OD – Users ■ NHLBI – AD ■ NIDA(NSC) – NIDA (Technology unknown) ■ NEI – NEI Clients
Delegation of Management	■ OD – Admins	■ OD – Users

	■ NHLBI – eDirectory	■ NHLBI – eDirectory, AD, Exchange

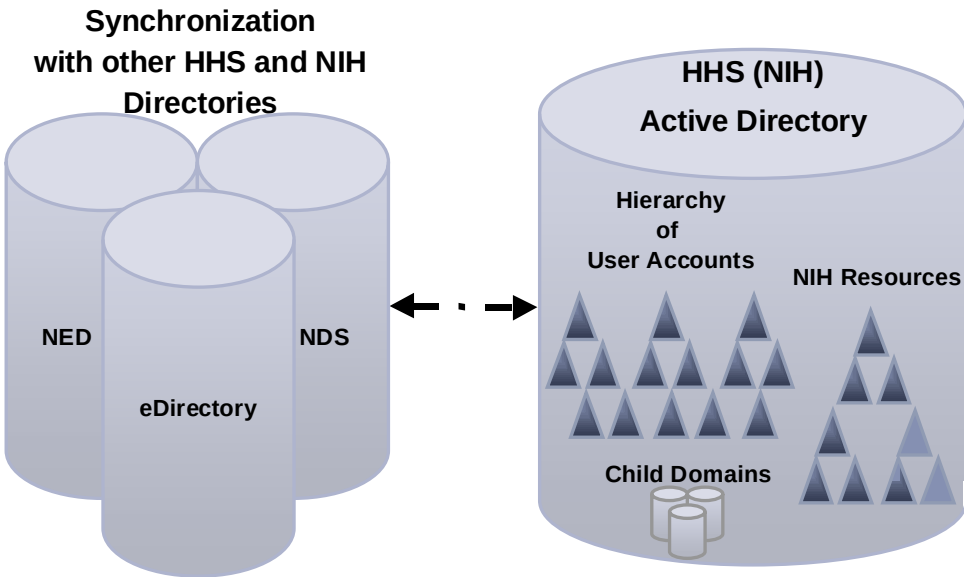
At a high level, Directory Services are used to perform Application Authorization, Password Synchronization, Directory Synchronization, DNS Services and User Policy information. Very few ICs are using Directory Services to facilitate the Delegation of Authority. Additional in-depth analysis will be required to determine if directories within NIH are performing other services.

5.0 NIH Active Directory Pattern

Description and Context

The Collaboration Domain Team produced a future-state Active Directory pattern called NIH Enterprise Active Directory. The NIH Enterprise Active Directory is a shared enterprise directory for NIH within the DHHS Forest. NIH is a multi-faceted enterprise serving a broad range of customers. This diversity in constituents prevents the use of a single directory system, as no single system meets all of NIH's needs.

Figure 4. Active Directory Logical Model



Collaboration Domain Team Meeting 18 – 16 May 2003

Currently, data synchronization between directories is accomplished through custom rule development (NED) or through third party developed software (eDirectory). As a result of the current migration project, from NT 4.0 to Active Directory, and the email consolidation project, Exchange 5.5 to Exchange 2000, NT 4.o domains and Exchange 5,5 directories will consolidated into a single NIH Active Directory.

Business and IT Drivers

- Emerging enterprise applications (e.g., Exchange 2000, New Business Systems)
- Network Services NIH Login (Single Sign-On)
- Reduction of complexity and network administration expenses.

Approach

The NIH Enterprise Active Directory is an Active Directory Service that serves the DHHS Active Directory Forest. Other directories within NIH can interface with Active Directory using various synchronization schemes.

Benefits

- Provides an NIH-wide representation of resources and user accounts
- Reduces management complexity and overall costs
- Provides a standard interface and data elements for consistent, comprehensive access to user account and resource data.

Limitations

- May constrain the flexibility for some ICs to extend the schema
- May disrupt informal support networks.

Assumptions

- Active Directory will be the Authoritative Data Source for user login information.

5.1 Logical AD Representation of the Future State

NIH is a multi-faceted enterprise serving a broad range of customers. This diversity in constituents prevents the use of a single directory system, as no single system meets all of NIH's needs. Systems in use at NIH should therefore be able to communicate with a minimum amount of effort. In the logical representation developed by the Collaboration Team, AD will interface with many different directories in place at NIH. This flexibility will be augmented by the data standards shown in Appendix B. The adoption of data standards will improve the portability of information between directories.

6.0 Enterprise NOS Bricks

The Collaboration Domain Team has developed a single brick detailing the enterprise NOS: Enterprise Directories.

These two bricks are used to better describe the consolidated collaboration patterns. To provide improved fidelity in the mainstream brick category, the category was divided into Tactical (0-2 years) and Strategic (2-5 years) time frames. Often NIH focuses on tactical solutions using the emerging technology space at NIH to test strategic technologies.

6.1 Enterprise Directories

Directories used in conjunction with the enterprise messaging systems:

Table 12. Enterprise Directories

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ eDirectory ■ AD ■ NDS ■ Exchange 5.5 ■ NT 4.0 Domains ■ PH ■ NED	■ eDirectory ■ Active Directory (AD) ■ NED	■ Meta Directory Technology
Retirement Targets (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
■ NT 4.0 Domains ■ NDS ■ PH	■ NDS ■ Exchange 5.5	■ Meta Directory Technology ■ Microsoft Meta Directory Services (MMS) 2003 ■ Oblix ■ AD Application Mode (ADAM)
Comments		
■ NIH has a de facto standard with eDirectory and AD. AD is the NOS of NIH, with eDirectory playing an important role for some large ICs within NIH. ■ See Data Standards in Appendix B. ■ Some additional areas of concern: ❑ A DNS (AD) requirement ❑ Multiple management applications and processes ❑ Multiple schemas ❑ Platform limitations ❑ Lack of standardization for directory and application development. June 11, 2003		

7.0 Enterprise Collaboration Bricks

The Collaboration Domain Team captured additional information, which was distilled into the following brick detailing a different segment of the Data & Information Technology taxonomy.

7.1 Collaboration Tools

Collaboration tools used within NIH:

Table 13. Collaboration Tools

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ Key Flow ■ Shared Folders (Exchange 5.5) ■ Plumtree ■ Share Point ■ WebX ■ Place Ware ■ Groove ■ eRoom ■ Project Server ■ Conference Server ■ WebDAV ■ Exchange 5.5 ■ AMBIS ■ GroupWise	■ Key Flow ■ Exchange 2000 ■ Plumtree ■ Share Point ■ WebX ■ Place Ware ■ Groove ■ eRoom ■ Project Server ■ Conference Server ■ WebDAV	■ TBD
Retirement Targets (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
■ GroupWise	■ Exchange 5.5 ■ AMBIS	■ None
Comments		
■ NIH is determining its collaboration needs. As such, a number of software packages are being reviewed.		
11 June 2003		

7.2 Problem Management Systems

The Collaboration Domain Team's data collection effort uncovered problem management systems used within NIH as collaboration tools. Both Remedy and HEAT were used in this manner. Duplication in problem management systems can often lead to additional expense as the systems are integrated. It is Gartner's recommendation that this area be examined to determine if the proper processes are being used to meet these data sharing and collaboration needs.

8.0 Next Actions

Listed below are other topics, as identified by the Collaboration Domain Team, for NIH to explore in follow-on Collaboration Architecture efforts:

- Explore Collaboration Products, in more detail
  - Data Collection Effort and Comparison
  - Collaboration Tool Selection Process for NIH
- Authoritative Data Source (People)
  - NIH Enterprise Directory (Alternatives)
  - Technologies
  - Business Processes
- Real Time Communications
  - Video, Voice, Data, Chat and Convergence
  - Wireless Devices and Applications
- Authorization Standards
  - Groups
- Spam Filtering
  - ORIM Policy
  - Client and/or Server Level
  - At NIH, IC or Personnel Level
- Foster Communication Between ICs About Extension Systems
  - “Show and Tell” and “Brown Bag” Sharing of Knowledge.

Appendix A—Glossary of Terms

Appendix A—Glossary of Terms

Term	Definition
Active Directory	The "directory service" portion of the Windows 2000 operating system. Active Directory manages the identities and relationships of the distributed resources that make up a network environment. It stores information about network-based entities (e.g., applications, files, printers and people) and provides a consistent way to name, describe, locate, access, manage and secure information about these resources. It the central authority that manages the identities and brokers the relationships between these distributed resources, enabling them to work together.
client	A system or a program that requests the activity of one or more other systems or programs, called servers, to accomplish specific tasks. In a client/server environment, the workstation is usually the client.
client/server	The splitting of an application into tasks performed on separate computers connected over a network. In most cases, the "client" is a desktop computing device (e.g., a PC) or a program "served" by another networked computing device (i.e., the "server"). Gartner has defined five styles of client/server computing, based on how presentation, application logic and data management functions are partitioned between the client and server device — see separate definitions for "distributed presentation," "remote presentation," "distributed function," "remote data management" and "distributed data management."
messaging	In e-mail, messaging consists of moving messages from user to user, application to application or place to place, providing a service analogous to that of the paper postal service and providing an infrastructure along which many other objects may be moved. The term is sometimes applied, with an entirely different meaning, to real-time interprocess communications in a transaction-processing environment.
OS (operating system)	The operating system is the main control program that runs a computer and sets the standard for running application programs. It is the first program loaded when the computer is turned on, and it resides in memory at all times. An operating system is responsible for functions such as memory allocation, managing programs and errors, and directing input and output. It may be developed by the computer vendor or by a third-party independent software vendor.
problem management	The core function of a customer service and support (CSS) application used by call centers. It coordinates a multitier, multiowner service and support environment, enables pattern analysis, provides management reports, and facilitates requesting additional service and support resources by providing hard numbers on the service workload and its changing nature. Because PM tools can also track service-level agreements (SLAs), they are valuable for monitoring compliance.
protocol	A set of procedures in telecommunications connections that the terminals or nodes use to send signals back and forth. Transmission Control Protocol/Internet Protocol (TCP/IP) is the standard protocol for the Internet and related networks such as intranets and extranets. Local-area networks (LANs) often rely on a different protocol. Networks and systems cannot communicate unless they use the same protocol or make use of a gateway.
server	A system or a program that receives requests from one or more client systems or programs to perform activities that allow the client to

Term	Definition
	accomplish certain tasks. The term is usually applied to computers that provide specific services to other computers on a network. Routing servers connect subnetworks of like architecture; gateway servers connect networks of different architectures by performing protocol conversions; and terminal, printer and file servers provide interfaces between peripheral devices and systems on the network.

Appendix B—Active Directory Data Standards

Appendix B: Active Directory Data Standards

The Collaboration Domain Team indentified seventeen fields as mandatory information fields for any Active Directory (AD) User Account. Each field is described in detail below.

Note: Quotations in examples are not part of the suggested value unless otherwise noted.

AD: User Account

An entry of this type represents a person that uses National Institutes of Health (NIH) resources and services including but not limited to current NIH employees, contractors, tenants of NIH facilities, participants in the NIH visiting programs, registered users of NIH computer facilities, grantees, reviewers, council members and collaborators.

1. Labeling Attributes

1.1 Display Name

Displayable name representative of individual in the format of [1.3 Last Name], [1.2 First Name] [1.4 Generation Qualifier] ([4.2 OpDiv Name]/[4.1 IC]).

Attribute Name: **Display-Name (AD)**
displayName (LDAP)

Max Length: **256**

Required: **Yes**

MultiValued: **False**

NED Attribute: **No direct match**

Example(s): **“Doe, James III (NIH/CIT)”**

1.2 First Name

Legal first name of person.

Attribute Name: **GivenName (AD)**
givenName (LDAP)

Max Length: **64**

MultiValued: **False**

NED Attribute: **1.3 Given Name**

Example(s): **“James”**

1.3 Last Name

Legal last name of person; does not include a generation qualifier.

Attribute Name: **Surname (AD)**
sn (LDAP)

Max Length: **64**

MultiValued: **False**

NED Attribute: **1.5 Surname**

Example(s): **“Doe”**

1.4 Generation Qualifier

Generation qualifier of person, if any, without periods.

Attribute Name: **Generation-Qualifier (AD)**
generationQualifier (LDAP)

Max Length: **64**

MultiValued: **False**

NED Attribute: **1.6 Generation Qualifier**

Example(s): **“Sr,” “Jr,” “III”**

1.5 NIH Unique Identifier