

Enterprise Directories Brick V1.0

Status of this Memo

This document proposes a refreshment of a technical standard for the National Institutes of Health (NIH) and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Table of Contents

1	Introduction.....	2
2	Description.....	2
3	Enterprise Directories	2
4	Contact.....	3
5	Changes.....	3
6	Author's Address	4
7	Summary of Comments.....	5

1 Introduction

This document updates the NIH Technical Architecture Standard for Enterprise Directories for the NIH community.

2 Description

Enterprise directories are electronic directories used to facilitate the search and discovery of related data in large data repositories quickly. Typical examples of electronic directories are email address directories such as the NIH email system and people directories such as NED. Making this data available electronically allows for high business value, while facilitating data quality by reducing the number of redundant sources of equivalent data.

3 Enterprise Directories

This brick provides baseline information and the future direction for deploying enterprise directories at NIH.

Table 1. Enterprise Directories

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
<ul style="list-style-type: none"> ■ AD Application Mode (ADAM) ■ Active Directory (COTS) ■ eDirectory ■ NIH Enterprise Directory (NED) ■ NDS 	<ul style="list-style-type: none"> ■ Active Directory (COTS) ■ NIH Enterprise Directory (NED) 	<ul style="list-style-type: none"> ■ Active Directory (COTS) ■ HSPD-12 driven initiatives
Retirement Targets (Technology to eliminate)	Containment (No new deployments)	Emerging (Technology to track)
<ul style="list-style-type: none"> ■ eDirectory 	<ul style="list-style-type: none"> ■ AD Application Mode (ADAM) ■ AD LDS (ADAM Replacement) ■ NDS 	<ul style="list-style-type: none"> ■ Identity Projects as part of HSPD-12 ■ Open Directory (Open Source) ■ Virtual Directories as part of large Application Suites (Oracle/Sun, Microsoft, IBM, or others)
Comments		
<ul style="list-style-type: none"> ■ Tactical and Strategic products were selected to leverage NIH's investment in products that are a proven fit for NIH's known future needs. Leveraging baseline products in the future will minimize the operations, maintenance, support and training costs for new products. ■ Some baseline products have been designated as Containment. These products are either not as widely or successfully deployed at NIH, or they do not provide as much functionality, value, or Total Cost of Ownership as low as the selected Tactical and Strategic products. ■ NIH has a de facto directory standard based on the use of Microsoft Active Directory. At NIH, Active Directory (AD) is the Network Operating System or NOS for NIH. NIH also currently uses an internal person data directory called NIH Enterprise Directory (NED). NED stores data about a person's contact information, location, and title for all people working at NIH. AD and NED also exchange information in order to keep the two directories consistent. More information can be found about NED at Http://ned.nih.gov ■ NIH is participating in several HSPD-12 related activities. This Homeland Security Directive will alter how NIH collects, lists, and uses data about people at NIH. 		

4 Contact

To contact the NIHRFC Editor, send an email message to EnterpriseArchitecture@mail.nih.gov

5 Changes

Version	Date	Change	Authority	Author of
---------	------	--------	-----------	-----------

				Change
0.1	12/06/09	Initiation		Joe Klosky
0.2	01/20/10	Minor formatting changes	NIHRFC0001	Kiley Ohlson
0.3	03/14/10	Integrated Comments and Responses	NIHRFC0001	Kiley Ohlson
0.4	03/21/10	Integrated changes requested by ITMC	NIHRFC0001	Joe Klosky
1.0	04/27/10	ARB Approved NIHRFC	ARB	Kiley Ohlson

6 Author's Address

Helen Schmitz / Joe Klosky
OD/Office of the Chief IT Architect, NIH
10401 Fernwood Road, Room 3NW10B
Bethesda, Maryland 20817-4800
Phone: 301-496-2328
Email: schmitzh@mail.nih.gov
Email: joe.klosky@nih.gov

7 Summary of Comments

Comment:

In this RFC, Active Directory Application Mode (ADAM) is in Containment, and *other virtual directories* are listed under Emerging Technologies to track in the future.

Just want to verify that we are not accidentally mixing up terminology or that there may be more to this that you have considered. ADAM is an extremely versatile and lightweight LDAP service (with minimal costs) that leverages Active Directory (AD). We frequently need to use ADAM for the flexibility it offers to meet unique requirements for various NIH applications – and help keep the NIH AD clean and secure. It is currently being used for Federation, and can be used to facilitate other initiatives in the future like Single Sign-on (SSO).

Response:

ADAM is a Windows server 2003 directory service tool that can run on any Windows 2003 server. ADAM has reached end of life by Microsoft. ADAM provides useful Active Directory light directory services to applications and processes. Due to its useful but light-weight nature, it's not recommended for wide spread use for enterprise directories at NIH. One of the largest complaints about ADAM is its need to leave a user logged in (it runs as a user service not a server service) for it to function. Please consult your ISSO if this is an acceptable operational practice or risk. Microsoft issued a replacement for ADAM called Active Directory Light-weight Directory Services (AD LDS) as part of Windows 2008. As with its predecessor ADAM, LDS is a lightweight directory service tool and not recommended for Enterprise directory services at this time.

<http://www.microsoft.com/windowsserver2003/lifecycle.msp>

Comment:

Baseline:
Add Active Directory Federation Services (ADFS)

Note: Applies To: Windows Server 2003 R2
Active Directory Federation Services (ADFS) is based on the emerging, industry-supported Web Services Architecture, which is defined in WS-* specifications. ADFS helps you use single sign-on (SSO) to authenticate users to multiple, related Web applications over the life of a single

online session. ADFS accomplishes this by securely sharing digital identity and entitlement rights across security and enterprise boundaries.

Tactical:

Add Active Directory Federation Services (ADFS)

Strategic:

Add Active Directory Federation Services (ADFS)

Add NIH Enterprise Directory (NED) - at this point there has been no mention of replacing NED in the next 2-5 years

Response:

Active Directory Federation Services (ADFS) is not an Enterprise Directory per se. ADFS is the facility to allow cross Active Directory domain authentication. This communications protocol is well suited for enabling Microsoft centric Single Sign-on capabilities at NIH due to our wide spread adoption of Active Directory as the prominent source for authentication (NIHnet and e-mail). While we think this technology enables Active Directory to better support end users directory needs,

[http://technet.microsoft.com/en-us/library/cc786469\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc786469(WS.10).aspx)