OD/ITAO
NIHRFC0051
Category: Standard

Helen Schmitz/ Joe Klosky
OD
January 2010

Identification and Authentication Brick
V1.0

Status of this Memo

This document updates a 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

This NIHRFC is an update to the enterprise standard for identification authentication tools used within the National Institutes of Health (NIH).

2 Background

This standard establishes NIH Login as the required method of implementing authentication in web-based applications at the NIH. Authenticated identities are the basis for many other information security services. Therefore, NIH needs to:

- Verify user identity as the basis for access control to NIH resource
- Control individual user access to the resources and services provided by those systems
- Create an audit trail of individual user access or attempted access to those systems, resources and services

Authentication services are crucial to access control and auditing services. If users' identities are not properly authenticated, NIH has no assurance that access to resources and services are properly controlled. In most situations, User ID and password combinations will provide an appropriate level of security if the User ID and password conform to NIH policy. However, NIH will implement stronger authentication for enterprise users with high system privileges (e.g. system, network and security administrators).

NIH Login shall be used by web-based applications for user authentication.

3 Changes to the Technology

There are no significant changes to the technology outlined in this brick. It is recommended that the date on the brick be updated to 2010 and re-published.

Table 1. Identification Authentication Brick

Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)	Emerging (Technology to track)
■ NIH Login	■ NIH Login	■ Biometrics which integrate with NIH Login ■ Smartcards which integrate with NIH Login
Containment (No new deployments)	**Retirement (Technology to eliminate)**	**Baseline Environment (As of last review)**
■ Application-specific user authentication based on databases including LDAP, RDBMSs ■ Application-specific user authentication including IP and MAC Addresses	■ None	■ Application-specific user authentication based on databases including LDAP, RDBMSs ■ Application-specific user authentication including IP and MAC Addresses ■ NIH Login (currently using CA SiteMinder)
Comments		
■ Tactical and Strategic products were selected to leverage NIH's investment in technologies 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. ■ As the purpose of this standard is to standardize Identification and Authentication for NIH applications through use of NIH Login, NIH Login is the only selection for Tactical and Strategic technologies and shall be used by new web-based applications requiring authentication functionality. ■ The NIH Login, itself, is the proposed standard and does not denote a specific supporting technology. ■ Currently, NIH Login utilizes CA SiteMinder		

4 Contact

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

5 Changes

Version	Change	Authority	Author of Change
0.1	Refresh of Brick		Helen Schmitz / Joe Klosky
0.2	Minor formatting changes	NIHRFC0001	Kiley Ohlson
0.3	Integrated Comments and Responses	NIHRFC0001	Kiley Ohlson
1.0	ARB Approved	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

7 Summary of Comments

Comment:

I have a question of clarification:
I believe we have a number of applications in our current baseline environment employing application-specific user authentication via Active Directory (e.g. SharePoint 2007 sites or other web applications internal to NIH using Integrated Windows Security).
These do not seem to be included in the tactical and strategic deployment section which only mentions NIH Login. Is there a reason why authentication via Integrated Windows Security/Active Directory is not included in the tactical section? Is the recommendation to move away from this authentication method for internal NIH applications? Or is this included and thought of as possible supporting technology of NIH Login?

Response:

Authentication as integrated in a COTS application, should consider NIH login in its design. Doing so will automatically elevate the application to PIV card enabled. If the Integrated authentication already allows for PIV card authentication then a cost benefit analysis may help IT system developers determine which scenario meets current and future end user needs.

Comment:

Smartcards should not only be in Emerging - this is now a requirement
Add Smartcards which integrate with NIH Login to Baseline, Tactical and Strategic

Response:

Yes, we agree, an important future state of authentication will retilize PIV cards. We will clarify the comments to ensure PIV type smartcards are clearly thought of as part of the NIH login environment. As a note, we feel the use of the term Smartcards are too broad for clear understanding at NIH. We believe the use of PIV cards, a subset of smart cards, is better due to the issues of smartcard technology in credit cards, and other forms. The emergence of contact-less smart cards also creates more smartcards sub-types and creates additional potential confusion.