Office of the Chief IT Architect
NRFC0014 /STD0008
Category: Standard

W. Jones and M. Silverman
CIT
June 2005

Staff Digital Certificate Brick
V1.0

Status of this Memo

This document specifies an NIH architectural standards track protocol for digital certificates issued to the NIH community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "National Institutes of Health Enterprise Architecture Standards Process" (NRFC0001/BCP0001) for the standardization state and status of this protocol. Distribution of this memo is intended for the NIH community.

Table of Contents

1 Introduction

The purpose of this NRFC is to establish a Staff Digital Certificate Brick as part of the NIH Enterprise Architecture. A **digital certificate** is a secure electronic document that certifies the identity of the individual assigned the certificate. Issued by a trusted third-party, the Certification Authority (CA), it contains the individual's name, public cryptographic key, and other related information. Digital certificates are used to support electronic authentication, digital signatures, and key management (i.e., encrypted email).

A **Staff Digital Certificate** is a digital certificate that is issued to an individual staff member of NIH. A **staff member** is defined as anyone who possesses a NIH issued Federal ID badge (e.g., employee, contractor, public health service member, etc.). The following digital certificates are outside the scope of this standard:

- Digital certificates issued to individuals outside of NIH,
- Digital certificates issued to other types of entities that are not staff members, including but not limited to web services and other devices), and
- Special purpose certificates (for example, those used to support the Microsoft® encrypted file system).

The Staff Digital Certificate Brick establishes the HHS Public Key Infrastructure (PKI) as the single tactical and strategic source of staff digital certificates at NIH. This standard is based on analysis of existing technologies in place at NIH coupled with HHS and Federal Public Key Infrastructure (PKI) policy requirements. HHS IRM Policy[1] on PKI requires that all Agencies within HHS operate within a single HHS-wide PKI trust domain that is cross-certified (i.e., interoperable) with the Federal Bridge Certification Authority (FBCA). OMB PKI policy[2] requires Federal Agencies to acquire digital certificates from a GSA qualified commercial shared service provider. The HHS PKI is the only solution that meets these requirements.

2 Staff Digital Certificates Brick

Baseline Environment (Today)	Tactical Deployment (0-2 years)	Strategic Deployment (2-5 years)
■ HHS PKI ■ Key Management System (KMS) ■ Microsoft .net CA ■ Other	■ HHS PKI	■ HHS PKI
Retirement Targets (Technology to eliminate)	**Containment (No new deployments)**	**Emerging (Technology to track)**
■ Key Management System (KMS)	■ Microsoft .net CA ■ All others	■ None

Comments

- 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.
- HHS policy dictates that HHS PKI digital certificates be deployed as User PKI certificates for all agencies within the department. Therefore, it is the only Tactical and Strategic solution for NIH.

3 References

[1] "HHS IRM Policy for Public Key Infrastructure (PKI) Certificate Authority (CA)." 8 January 2001. http://irm.cit.nih.gov/itmra/HHS-IRM-2000-0011.html (12 April 2005).

[2] Forman, Mark. "Streamlining Authentication and Identity Management within the Federal Government." Memorandum for the Chief Information Officers of Departments and Agencies. 3 July 2003. http://www.whitehouse.gov/omb/inforeg/eauth.pdf (12 April 2005).

For additional information about the NRFC process and/or the NIH Enterprise Architecture visit http://enterprisearchitecture.nih.gov.

For additional information on the HHS PKI Program visit http://www.pki.hhs.gov.

4 Contact

To contact the NRFC Editor, send an email message to EnterpriseArchitecture@mail.nih.gov. . To contact the authors, send an email message to wkj@mail.nih.gov or silvermm@mail.nih.gov.

5 Security Considerations

This NRFC raises no security issues.

6 Changes

Version	Change	Authority	Author of Change
0.1	Original Draft	NRFC0001/BCP0001	Bill Jones and Mark Silverman
1.0	Approved as standard	ARB 6/22/2005	Steve Thornton, NRFC Editor

7 Authors' Addresses

Bill Jones
National Institutes of Health
10401 Fernwood Road
MSC 4806
Bethesda, Maryland 20817
Phone: 301-402-1241
Email: wkj@mail.nih.gov

Mark Silverman
National Institutes of Health
10401 Fernwood Road
MSC 4806
Bethesda, Maryland 20817
Phone: 301-496-2317
Email: silvermm@mail.nih.gov