OCITA
NRFC0022
Category: Informational

M. Silverman
CIT
August 2006

Federal Authentication and Identity Management v1.0

Status of this Memo

This memo provides information for the NIH architecture community. This memo does not specify an NIH architecture standard of any kind. Distribution of this memo is unlimited.

Table of Contents

1 Introduction

It is a security principle of the NIH architecture that security controls will be based on a risk analysis and risk management decision. The NIH Enterprise Architecture identifies various authentication security controls in the Identification and Authentication Brick. The purpose of this NRFC is to identify the Federal standards and methodologies used to determine the level of risk assigned to an information technology (IT) system and the authentication mechanisms required for that particular level of risk.

This NRFC does not define any new concepts or requirements; it is simply a compilation of information presented across a number of Federal publications. The purpose of this NRFC is to provide a concise guide to Federal authentication and identity management requirements and to show how these requirements interrelate.

2 Federal Requirements

The National Institutes of Standards (NIST), Office of Management and Budget (OMB) and other Federal entities have promulgated a number of E-authentication and identity management standards and requirements. Section 2.1 below is an overview that traces the relationships between these various documents, with a primary focus on identifying the type of credential (e.g., password, PKI token, etc.) that must be used to access various IT systems and the requirements associated with issuing that particular credential. Section 2.2 provides a detailed summary of the key requirements identified in each document.

2.1 Overview

To see how all of these requirements documents tie together, start with FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems," which states that:

> **Organizations must employ all security controls in the respective security control baselines unless specific exceptions are allowed based on the tailoring guidance provided in NIST Special Publication 800-53.[1]**

NIST SP 800-53, "Recommended Security Controls for Federal Information Systems," defines security control IA-2, User Identification and Authentication, as follows:

> **NIST Special Publication 800-63 provides guidance on remote electronic authentication. For other than remote situations, when users identify and authenticate to information systems within a specified security perimeter which is considered to offer sufficient protection, NIST Special Publication 800-63 guidance should be applied as follows: (i) for low-impact information systems, tokens that**

meet Level 1, 2, 3, or 4 requirements are acceptable; (ii) for moderate-impact information systems, tokens that meet Level 2, 3, or 4 requirements are acceptable; and (iii) for high-impact information systems, tokens that meet Level 3 or 4 requirements are acceptable.[2]

NIST SP 800-53 effectively divides access to Federal IT systems into three categories:

1. **Internal systems** where all network access occurs within the firewall (a specified security perimeter). For these systems, their authentication requirements (Level 1, 2, 3 or 4), as defined in Table 2, are based upon the system's security classification (low, moderate or high impact), as defined in Table 4. These requirements are illustrated in table 1 below.

2. **External systems** where network access is granted to all Internet users (i.e., those outside the firewall). For these systems, their authentication requirements, as defined in Table 2, are based upon their E-Authentication risk assessment, as described in Table 3. These requirements are illustrated in Table 1 below.

3. **Remote access** where a user outside the firewall is granted access, through the use of dial-up connections or virtual private network technology, to systems not specifically designed for public access. In this case authentication must be performed in accordance with OMB M-06-16, "Protection of Sensitive Agency Information," which requires the use of **two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.[3]**

Credentials Required by Application Assurance Level					
Auth [1] Level	Security Classification of internal application [2]	Low	Moderate	High	
	Assurance level of external application [3]	1	2	3	4
1	Self-registered (e.g., public portal)	●			
2	Single factor authentication (e.g., password)	●	●		
3	Multi-factor authentication (e.g., SecurID)	●	●	●	
4	Strong cryptographic authentication (e.g., smartcard)	●	●	●	●

[1] See Table 2
[2] See Table 4
[3] See Table 3

Table 1: Required Credential by Assurance Level

Also driving Federal authentication requirements is Homeland Security Presidential Directive/Hspd-12, "Policy for a Common Identification Standard for Federal Employees and Contractors."[4] This directive mandates the use of a new credential (ID Badge) and requires its use by Federal employees and contractors "in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems." FIPS 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors" [5] defines the standard to be followed in issuing the credential (PIV-1), as well as the physical and technical characteristics of the credential (PIV-2).

Everyone issued a Federal ID badge must undergo a National Agency Check with Inquiries (NACI) background check, consistent with all non-sensitive public trust employees (see Table 5). The NACI includes:

- The standard National Agency Check (NAC) consisting of a Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), Federal Bureau of Investigation (FBI) Name Check, and FBI National Criminal History Fingerprint Check; and
- Written inquires and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).

Depending upon the position sensitivity level, as described in Table 5, additional background checking may be required.

Embedded within the smart chip of the new PIV-2 credential, is a digital certificate to be used to authenticate to Federal IT systems. This certificate must be issued by a certificate authority (CA) that has been cross-certified with the Federal Bridge CA (FBCA) at MEDIUM-HW or the HIGH Assurance Level, as described in Table 6. Use of the certificate, with the PIV-2 credential, meets Level 4 assurance requirements (Table 2).

2.2 Requirement Specifications

This section summarizes the salient points from the following Federal publications:

- NIST SP 800-63, "Electronic Authentication Guideline"[6]
- OMB M-04-04, "E-Authentication Guidance for Federal Agencies"[7]
- NIST FIPS Pub 199, "Standards for Security Categorization of Federal Information and Information Systems"[8]
- "HHS Personnel Security/Suitability Handbook"[9]
- FPKI "X.509 Certificate Policy For The Federal Bridge Certification Authority"[10]

Note that the tables in the following sections are color coded to relate the specific requirements document back to the overview Table 1: Required Credential by Assurance Level.

2.2.1 NIST SP 800-63 - Authentication Assurance Levels

Table 2, below, describes the four Federal authentication assurance levels (1-4) in terms of what types of authentication credentials (tokens) are required and the identity proofing requirements associated with those credentials.

<table>
<tr><th colspan="3">Authentication Assurance Levels</th></tr>
<tr><td>Description</td><td colspan="2">Assurance levels describe the degree of certainty that a user has presented an identifier (i.e., credential) that refers to his or her identity. In this context, assurance is defined as (1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and (2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.</td></tr>
<tr><td>Source</td><td colspan="2">SP 800-63, “Electronic Authentication Guideline.”
http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf.

See also: OMB M-04-04, “E-Authentication Guidance for Federal Agencies.”
http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf.</td></tr>
<tr><th>Designation</th><th>Description</th><th>Requirements</th></tr>
<tr><td rowspan="2">Level 1</td><td rowspan="2">Little or no confidence in the asserted identity’s validity.

The authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data.</td><td>Credential: any level 2, 3 or 4 credential.</td></tr>
<tr><td>Identity proofing: none</td></tr>
<tr><td rowspan="2">Level 2</td><td rowspan="2">Some confidence in the asserted identity’s validity.

Single factor remote network authentication.</td><td>Credential: any level 3 or 4 credential or a shared secret memorized by the claimant (e.g., password).</td></tr>
<tr><td>Identity proofing:
➢ In-person inspection/visual verification of valid current primary Government Picture ID that contains applicant’s picture, and either address of record or nationality (e.g. driver’s license or passport); or
➢ remote inspection of submitted documentation including Government Picture ID and a financial account number (e.g., checking account, savings account, loan or credit card) which can be independently verified through a record checks with either the applicable agency, institution, credit bureau or similar databases; plus a notice is sent to the address of record or credential is issued in a manner that confirms the address of record.</td></tr>
</table>

Level 3	High confidence in the asserted identity's validity. Multi-factor remote network authentication.	*Credential:* any level 4 credential **or** a software cryptographic token (e.g., digital certificate) combined with a password or biometric **or** a one-time password device combined with a password or biometric (e.g., SecurID + PIN).
		Identity proofing: ➢ In-person inspection of valid current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport), plus verification via the issuing government agency or through credit bureaus or similar databases, confirming that: name, DoB, address and other personal information in record are consistent with the application; **or** ➢ remote inspection of submitted documentation including Government Picture ID and a financial account number (e.g., checking account, savings account, loan or credit card) which can be independently verified through a record checks with either the applicable agency, institution, credit bureau or similar databases; plus credential must be issued in a manner that confirms the address of record.
Level 4	Very high confidence in the asserted identity's validity. Strong cryptographic authentication of all parties and all sensitive data transfers between the parties.	*Credential:* hardware cryptographic token (i.e., smartcard) that is activated/protected by a password or biometric.
		Identity proofing must be done in-person and includes the inspection and verification of two independent ID documents or accounts, meeting the requirements of Level 3 (in-person and remote), one of which must be current primary Government Picture ID that contains applicant's picture, and either address of record or nationality (e.g. driver's license or passport), and a recording of a biometric of the applicant at the time of application.

Table 2: E-Authentication Security Levels

2.2.2 OMB M-04-04 - Requirements for Externally Facing Applications

Table 3, below, describes how the four Federal authentication assurance levels (1-4) should be applied in authenticating users of externally facing (i.e., public) applications.

Externally Facing Application Assurance Levels					
Description	The assurance level required by an externally facing application is obtained by considering all of the potential direct and indirect results of an authentication failure (i.e., risk assessment). The maximum potential risk, for each category and assurance level, is noted below.				
Source	OMB M-04-04, "E-Authentication Guidance for Federal Agencies" http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf.				
Potential Impact of Authentication Errors		**Level 1**	**Level 2**	**Level 3**	**Level 4**
Inconvenience, distress, reputation		Low	Moderate	Moderate	High
Financial loss or agency liability		Low	Moderate	Moderate	High
Harm to agency program or public interests		--	Low	Moderate	High
Unauthorized release of sensitive information		--	Low	Moderate	High
Civil or criminal violations		--	Low	Moderate	High
Personal safety		--	--	Low	Moderate

Table 3: External Application Assurance Levels

To assist Agencies in performing authentication risk assessments, the Federal E-Authentication Initiative teamed with the Software Engineering Institute (SEI) at Carnegie Mellon University to develop the Electronic Risk and Requirements Assessment (e-RA) toolkit, which can be found at: http://www.cio.gov/eauthentication/era.htm.

2.2.3 NIST FIPS 199 - Security Categorization of IT Systems

Table 4, below, describes how to identify an IT system as either Low, Moderate or High risk.

Categorization of Information and Information Systems	
Description	Standard used by federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels. The security categories are based on the potential impact to an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.
Source	FIPS Pub 199, "Standards for Security Categorization of Federal Information and Information Systems." http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.
Designation	Description
LOW	The loss of confidentiality, integrity, or availability could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
MODERATE	The loss of confidentiality, integrity, or availability could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
HIGH	The loss of confidentiality, integrity, or availability could be expected to have a ***severe or catastrophic*** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Table 4: IT System Security Categories

2.2.4 HHS - Position Sensitivity Levels

Table 5, below, describes the position sensitivity level designations for Federal staff.

Position Sensitivity Levels		
Description	There are three position sensitivity designations (Non-Sensitive, Public Trust, and National Security) which correlate with six specific sensitivity levels (Levels 1 through 6).	
Source	"HHS Personnel Security/Suitability Handbook," http://www.hhs.gov/ohr/manual/pssh.pdf.	
Designation	Description	Investigation Requirements
Level 1	Non-Sensitive	NACI (name & fingerprint checks & written inquiries), except for Intermittent, seasonal, per-diem, or temporary positions that do not exceed an aggregate of 180 days in either a single continuous or series of appointments and Aliens employed outside the US.
National Security Positions (levels 2 – 4)	National Security Positions are those in which the incumbent needs a security clearance for access to classified national security information.	
Level 2	Non-Critical Sensitive, requires a CONFIDENTIAL or SECRET clearance.	ANACI (Access NACI)
Level 3	Critical-Sensitive, requires a TOP SECRET or (DOE's) Q clearance.	SSBI (Single Scope Background Investigation)
Level 4	Special-Sensitive, requiring Special Access (or Presidential Appointee)	SSBI (Single Scope Background Investigation)
Public Trust Positions (levels 5 -6)	Public Trust Positions are those requiring a much higher degree of integrity with unwavering public confidence in the individual occupying the position. Public trust positions include positions encumbered by the following officials: (not all-inclusive) SES members, Schedule C appointees, administrative law judges, most commissioned corp officers, GS-13 to 15 officials who are substantially involved in contracts, procurements, grants, or responsibilities involving a high risk for conflict of interest. Public trust positions also include individuals with the following duties: law enforcement, investigations, audit, security, and access to sensitive, proprietary, or financial information, including access through, and/or control over, automated information systems (computer data systems).	
Level 5	Position holds moderate relative risk as determined by management	NACIC (NACI + credit check)
Level 6	Position holds high risk as determined by management	BI (Background Investigation)

Table 5: Position Sensitivity Levels

2.2.5 Federal PKI Assurance Levels

Table 6, below, describes the assurance levels of digital certificates issued by PKIs that are cross-certified with the Federal Bridge Certificate Authority (FBCA) and the identity proofing and CA operational requirements associated with each level.

FBCA Assurance Levels		
Description	The Federal Bridge Certification Authority (FBCA) assurance levels define the operational requirements (i.e., Certificate Policy) that must be followed by a PKI Certificate Authority (CA) that is cross-certified with the FBCA. Cross-certification with the FBCA establishes a common trust relationship between all CAs that are cross-certified with the FBCA and, by extension, between all holders of digital certificates issued by those CAs. Within each digital certificate is a policy identifier indicating the specific policy (assurance level) that governs how that certificate was issued, which in turn provides the recipient of the certificate (relying party) an indication of how much that certificate should be trusted as an assertion of identity.	
Source	"X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)." http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf.	
Designation	Description	Requirements
RUDIMENTARY	This level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication, and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.	No identification requirement; applicant may apply and receive a certificate by providing his or her e-mail address. Very lax CA security controls and procedures.
BASIC	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.	Identity established by in-person proofing or remotely verifying information provided by applicant including ID number and account number through record checks with the applicable agency or institution, through credit bureaus or similar databases. Credentials issued in a manner that confirms address of record.

MEDIUM	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.	Identity shall be established by in-person proofing or by an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent (e.g., Notary Republic) may suffice as meeting the in-person identity proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License). CA security controls and procedures are more stringent than BASIC.
MEDIUM-HW	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.	Requirements are identical to those defined for MEDIUM, with the exception that the subscriber must use a FIPS 140-2 cryptographic module (e.g., smartcard).
MEDIUM-CBP (commercial best practice)	Same as MEDIUM	Requirements are identical to MEDIUM with the exception that there is no there is no citizenship requirement for being in a trusted role.
MEDIUM-HW-CBP	Same as MEDIUM-HW	Requirements are identical to MEDIUM-HW, with the exception that there is no there is no citizenship requirement for being in a trusted role.
HIGH	This level is reserved for cross-certification with government entities and is appropriate for those environments where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.	Identity established by in-person proofing and information provided shall be checked to ensure legitimacy Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License). Subscriber must use a FIPS 140-2 cryptographic module (e.g., smartcard). CA security controls and procedures are more stringent than MEDIUM.

Table 6: FBCA PKI Assurance Levels

3 References

1. National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 200: Minimum Security Requirements for Federal Information and Information Systems*. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf. March 2006. Page 65.

2. Ross, Ron, et al; National Institute of Standards and Technology (NIST). *Special Publication 800-53: Recommended Security Controls for Federal Information Systems*. http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf. February 2005. Page 4.

3. Johnson, Clay, Director, Office of Management and Budget (OMB). *M-06-16: Protection of Sensitive Agency Information*. http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf. June 23, 2006.

4. Bush, George W., President of the United States of America. Homeland Security Presidential Directive/HSPD-12: Policy for a Common Identification Standard for Federal Employees and Contractors. http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html. August 27, 2004.

5. National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 201: Personal Identity Verification (PIV) of Federal Employees and Contractors.* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-v5.pdf . March 2006.

6. Burr, Bill; Polk, Tim and Dodson Dona; National Institute of Standards and Technology (NIST). *Special Publication 800-63: Electronic Authentication Guideline.* http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf. April 2006

7. Bolten, Joshua B., Director, Office of Management and Budget (OMB). *M-04-04: E-Authentication Guidance for Federal Agencies*. http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf. December 16, 2003.

8. National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems.* http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. February 2004.

9. Department of Health and Human Services. *Personnel Security/Suitability Handbook*. http://www.hhs.gov/ohr/manual/pssh.pdf. January 1998.

10. Federal Public Key Infrastructure Policy Authority. *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA).* http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf. January 12, 2006.

4 Contact

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

5 Security Considerations

All Federal IT systems are required to meet the authentication risk assessment and credential specifications identified in this NRFC.

6 Changes

Version	Date	Change	Authority	Author of Change
0.1	6/15/06	Original Document	NRFC0001/BCP0001	Mark Silverman
0.2	6/28/06	-Assigned NRFC number -corrected organizational identifier -Formatting changes -Minor copy edits -Corrected broken links	NRFC0001	Steve Thornton, NRFC Editor
0.3	6/28/06	Minor edits		Mark Silverman
0.4	8/17/06	- Added reference to M-06-16 - Added reference to e-RA toolkit - Minor edits		Mark Silverman
1.0	8/31/2006	-Approved by Chief IT Architect	NRFC0001 and Chief IT Architect	Steve Thornton

7 Author's Address

Mark Silverman
Center for Information Technology
10401 Fernwood Road, Room 3D11
Bethesda, Maryland 20817-4800
Phone: 301-496-2317
Email: mls@nih.gov