United States

Office of Personnel Management (OPM)

Electronic Signature Standards and Requirements

February 2013

Version 1.0

OPM Electronic Signature Standards and Requirements

Contents

Introduction 3

Standards 3

Risk Assessment 3

Determining Potential Impact of Authentication Errors: 4

Potential impact of inconvenience, distress, or damage to standing or reputation: 4

Potential impact of financial loss: 4

Potential impact of harm to agency programs or public interests: 4

Potential impact of unauthorized release of sensitive information: 4

Potential impact to personal safety: 5

The potential impact of civil or criminal violations is: 5

Determining Assurance Level: 5

Assurance Level Standards 6

Not Applicable (Negligible) 6

Low Impact 6

Moderate Impact 7

High Impact 7

Criteria 8

Checklist 9

Certification 9

References 9

Introduction

This document serves as the standards and requirements that program offices and contractors must comply with in the implementation of electronic signatures on Office of Personnel Management electronic information systems.

Standards

OPM's standards for electronic signatures are adapted from and consistent with Government-wide guidance for defining electronic signature risk and assurance levels provided by the Office of Management and Budget, the National Institute of Standards and Technology, and the Department of the Treasury. Program offices must perform a risk assessment against the following standards to determine the requirements for their electronic signature solution.

Risk Assessment

Program offices must assess the potential risks associated with electronic signatures and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:

a) potential harm or impact, and
b) the *likelihood* of such harm or impact.

Categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations.

Required assurance levels for electronic signatures are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." The potential impact values are:

- Not applicable (negligible)
- Low impact
- Moderate impact
- High impact

The next section defines the potential impacts for each category. Note: If authentication errors cause no measurable consequences for a category, there is "no" impact.

Determining Potential Impact of Authentication Errors:

Potential impact of inconvenience, distress, or damage to standing or reputation:

- Low—at worst, limited, short-term inconvenience, distress or embarrassment to any party.
- Moderate—at worst, serious short term or limited long-term inconvenience, distress or damage to the standing or reputation of any party.
- High—severe or serious long-term inconvenience, distress or damage to the standing or reputation of any party (ordinarily reserved for situations with particularly severe effects or which affect many individuals).

Potential impact of financial loss:

- Low—at worst, an insignificant or inconsequential unrecoverable financial loss to any party, or at worst, an insignificant or inconsequential agency liability.
- Moderate—at worst, a serious unrecoverable financial loss to any party, or a serious agency liability.
- High—severe or catastrophic unrecoverable financial loss to any party; or severe or catastrophic agency liability.

Potential impact of harm to agency programs or public interests:

- Low—at worst, a limited adverse effect on organizational operations or assets, or public interests. Examples of limited adverse effects are: (i) mission capability degradation to the extent and duration that the organization is able to perform its primary functions with noticeably reduced effectiveness, or (ii) minor damage to organizational assets or public interests.
- Moderate—at worst, a serious adverse effect on organizational operations or assets, or public interests. Examples of serious adverse effects are: (i) significant mission capability degradation to the extent and duration that the organization is able to perform its primary functions with significantly reduced effectiveness; or (ii) significant damage to organizational assets or public interests.
- High—a severe or catastrophic adverse effect on organizational operations or assets, or public interests. Examples of severe or catastrophic effects are: (i) severe mission capability degradation or loss of to the extent and duration that the organization is unable to perform one or more of its primary functions; or (ii) major damage to organizational assets or public interests.

Potential impact of unauthorized release of sensitive information:

- Low—at worst, a limited release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in a loss of confidentiality with a low impact as defined in FIPS PUB 199.
- Moderate—at worst, a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a moderate impact as defined in FIPS PUB 199.
- High—a release of personal, U.S. government sensitive, or commercially sensitive information to unauthorized parties resulting in loss of confidentiality with a high impact as defined in FIPS PUB 199.

Potential impact to personal safety:

- Low—at worst, minor injury not requiring medical treatment.
- Moderate—at worst, moderate risk of minor injury or limited risk of injury requiring medical treatment.
- High—a risk of serious injury or death.

The potential impact of civil or criminal violations is:

- Low—at worst, a risk of civil or criminal violations of a nature that would not ordinarily be subject to enforcement efforts.
- Moderate—at worst, a risk of civil or criminal violations that may be subject to enforcement efforts.
- High—a risk of civil or criminal violations that are of special importance to enforcement programs.

Determining Assurance Level:

Compare the impact profile from the risk assessment to the impact profiles associated with each assurance level, as shown in Table 1 below. To determine the required assurance level, find the lowest level whose impact profile meets or exceeds the potential impact for every category analyzed in the risk assessment. Thus, if five categories of potential impact are appropriate for the negligible level, and one category of potential impact is appropriate for the low impact level, the transaction would require a low impact level authentication. For example, if the misuse of a user's electronic identity/credentials during a medical procedure presents a risk of serious injury or death, map to the risk profile identified under the high impact level, even if other consequences are minimal.

Table 1 – Maximum Potential Impacts for Each Assurance Level

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**Not Applicable**	**Low Impact**	**Moderate Impact**	**High Impact**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

In analyzing potential risks, the program office must consider all of the potential direct and indirect results of an authentication failure, including the possibility that there will be more than one failure, or harms to more than one person. The definitions of potential impacts contain some relative terms, like "serious" or "minor," whose meaning will depend on context. The program should consider the context and the nature of the persons or entities affected to decide the relative significance of these harms. The

analysis of harms to agency programs or other public interests depends strongly on the context; the program office should consider these issues with care. In some cases (as shown in Table 1), impact may correspond to multiple assurance levels. For example, Table 1 shows that a moderate risk of financial loss corresponds to assurance levels low impact and moderate impact. In such cases, program offices should use the context to determine the appropriate assurance level.

Assurance Level Standards

After completing a risk assessment and mapping the identified risks to the required assurance level, program offices can select appropriate technology that, at a minimum, meets the technical requirements for the required level of assurance. In particular, there are technical requirements for each of the four levels of assurance in the following areas:

- Tokens (typically a cryptographic key or password) for proving identity,
- Identity proofing, registration and the delivery of credentials which bind an identity to a token,
- Remote authentication mechanisms, that is the combination of credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be,
- Assertion mechanisms used to communicate the results of a remote authentication to other parties.

A summary of the technical requirements for each of the four risk impact levels is provided below. For more details, please refer to the National Institute of Standards and Technology's "Electronic Authentication Guideline," Section 8.2.

Not Applicable (Negligible) – Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of three other impact levels. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Plaintext passwords or secrets are not transmitted across a network at this level. However this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed. In many cases an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.

At the negligible impact level, long-term shared authentication secrets may be revealed to verifiers. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Low Impact – This level requires single factor remote network authentication. At low impact level, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at this level. It

allows any of the token methods of moderate impact and high impact levels, as well as passwords and PINs. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Eavesdropper, replay, and on-line guessing attacks are prevented.

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the Credentials Service Provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are required. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

Moderate Impact – This level requires multi-factor remote network authentication. At this level, identity proofing procedures require verification of identifying materials and information. Moderate impact authentication is based on proof of possession of a key or a one-time password through a cryptographic protocol. Moderate impact authentication requires cryptographic strength mechanisms that protect the primary authentication token (secret key, private key or onetime password) against compromise by the protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. A minimum of two authentication factors is required. Three kinds of tokens may be used: “soft” cryptographic tokens, “hard” cryptographic tokens and “one-time password” device tokens.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token, and must first unlock the token with a password or biometric, or must also use a password in a secure authentication protocol, to establish two factor authentication. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Approved cryptographic techniques are used for all operations. Assertions issued about claimants as a result of a successful authentication are either cryptographically authenticated by relying parties (using Approved methods), or are obtained directly from a trusted party via a secure authentication protocol.

High Impact – This level is required to have the highest practical remote network authentication assurance. High impact authentication is based on proof of possession of a key through a cryptographic protocol. High impact level is similar to moderate impact level except that only “hard” cryptographic tokens are allowed, FIPS 140-2 cryptographic module validation requirements are strengthened, and subsequent critical data transfers must be authenticated via a key bound to the authentication process. The token shall be a hardware cryptographic module validated at FIPS 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. By requiring a physical token, which cannot readily be copied and since FIPS 140-2 requires operator authentication at Level 2 and higher, this level ensures good, two factor remote authentication.

High impact level requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The protocol threats including: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks are prevented. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the Credentials Service Provider (CSP), however session (temporary) shared secrets may be provided to independent verifiers by the CSP. Strong Approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

Criteria

In order to adopt an electronic signature solution, a program office or contractor must:

1. Examine current business process that is being considered for conversion to employ electronic documents, forms, or transactions, identifying customer needs and demands as well as the existing risks associated with fraud, error, or misuse.

2. Evaluate the risk level of the business process and transactions in accordance to the standards set in the Standards section of this document, which are adapted and compliant with OMB and NIST guidance. These risk levels are: not applicable, low, medium, and high.

3. Based on the risk level determined, identify the corresponding authentication standard required as outlined in Assurance Level Standards subsection of the Standards section of this document.

4. Evaluate how each electronic signature alternative can meet the required standards and may minimize risk compared to the costs incurred in adopting an alternative.

5. Review and assess proposed electronic signature technology, and submit the assessment to the program office and Chief IT Architect in the Office of the Chief Information Officer for review and recommendation to the CIO.

6. Develop plans for retaining and disposing of information, ensuring that it can be made continuously available to those who will need it, for managerial control of sensitive data and accommodating changes in staffing, and for adherence to these plans. Refer to Records Management Guidance for Agencies Implementing Electronic Signature Technologies issued by NARA. Also consult regulations promulgated by NARA regarding Standards for Creation, Use, Preservation and Disposition of Electronic Records at 36 CFR subparts A, B, and C.

7. Develop management strategies to provide appropriate security for physical access to electronic records.

8. Determine if regulations or policies are adequate to support electronic transactions and record keeping, or if “terms and conditions” agreements are needed for the particular application. If new regulations or policies are necessary, disseminate them as appropriate.

9. Conduct a final validation to confirm that the system achieves the required assurance level for the user-to-agency process. The program office should validate that the authentication process satisfies the systems' authentication requirements as part of required security procedures (e.g., certification and accreditation).

10. Implement the selected technology to the information collection system.

Checklist

- ✓ Program office examined current business process and determined that employing electronic signatures was viable and practicable.
- ✓ Program office completed risk assessment in accordance to the standards set forth in this document.
- ✓ Program office determined the risk impact level of the use of electronic signatures
- ✓ Program office considered the various technology choices available that met the standards set forth in this document and determined the appropriate selection for the business process in question.
- ✓ Program office provided their selection to the Chief IT Architect for referral and approval of the CIO.
- ✓ Program office developed records management plans for the electronic signature solution in accordance to "Records Management Guidance for Agencies Implementing Electronic Signature Technologies" issued by NARA.
- ✓ Program office conducted final validation of system to assure standards are met.
- ✓ Program office implanted the electronic signature solution

Certification

Program offices must submit their proposed electronic signature solution to the Chief IT Architect for approval by the CIO.

Program offices must periodically reassess the information system to ensure that the electronic signature requirements continue to be valid as a result of technology changes or changes to the OPM's business processes. Program offices may adjust the electronic signature solution's level of assurance using additional risk mitigation measures.

References

E-Authentication Guidance for Federal Agencies, OMB Memorandum M-04-04, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

Electronic Authentication Guideline, NIST Special Publication 800-63, Version 1.0.2, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

Electronic Authentication Policy, Department of the Treasury, 66 FR 394, http://www.gpo.gov/fdsys/pkg/FR-2001-01-03/pdf/01-79.pdf

Implementation of the Government Paperwork Elimination Act, Office of Management and Budget, http://www.whitehouse.gov/omb/fedreg_gpea2