ITL BULLETIN FOR DECEMBER 2011

REVISED GUIDELINE FOR ELECTRONIC AUTHENTICATION OF USERS HELPS ORGANIZATIONS PROTECT THE SECURITY OF THEIR INFORMATION SYSTEMS

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Individuals and organizations conducting electronic transactions with the federal government benefit when they have quick and easy access to government online services over open networks. Federal agencies need a level of assurance about the identity of these remote users in order to protect the security of their information systems and the privacy of individuals.

Electronic authentication (e-authentication) is the process of establishing confidence in the information that users present electronically to identify themselves to an information system. The electronic authentication of individuals conducting government business presents difficult technical challenges to organizations when the authentication procedures and the transactions take place over open networks, and system security and privacy must be protected.

To assist organizations in addressing these challenges, the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently issued Special Publication (SP) 800-63-1, *Electronic Authentication Guideline.* This revised guideline, which supersedes an earlier guideline, NIST SP 800-63, updates information about and recommendations for the secure implementation of electronic authentication methods, reflecting changing technology and current uses of e-authentication techniques.

Use of E-Authentication Methods by Federal Agencies

The Office of Management and Budget (OMB) issued Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, to help federal agencies provide secure electronic services that protect individual privacy. The memorandum advises agencies to review their electronic transactions, determine which transactions require e-authentication, and provide an appropriate level of assurance for those transactions that require electronic authentication. M-04-04 describes four levels of identity assurance and references NIST technical standards and guidelines, which are developed for agencies to use in identifying the appropriate authentication technologies that meet their requirements.

OMB M-04-04 defines four levels of assurance, Levels 1 to 4, in terms of the consequences of authentication errors and misuse of identification credentials:

Level 1 - Little or no confidence in the asserted identity's validity;
Level 2 - Some confidence in the asserted identity's validity;
Level 3 - High confidence in the asserted identity's validity; and
Level 4 - Very high confidence in the asserted identity's validity.

OMB defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with the criteria for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and the likelihood of occurrence of each application or transaction.

OMB outlines a five-step process that agencies should apply to meet their e-authentication assurance requirements:

1. Conduct a risk assessment of the government system. A risk assessment tool (available here) is an example of a suitable tool and methodology. Also, NIST SP 800-30, *Risk Management Guide for Information Technology Systems,* offers a general process for risk assessment and risk mitigation.

2. Map identified risks to the appropriate assurance level. The risk from an authentication error is a function of two factors: potential harm or impact and 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; and
- Civil or criminal violations.

Required assurance levels for electronic transactions 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.*

3. Select technology based on e-authentication technical guidance. After the appropriate assurance level has been determined, OMB directs agencies to select technologies that meet the corresponding technical requirements, as specified in NIST SP 800-63-1, *Electronic Authentication Guideline*. Agencies implementing existing e-authentication technology should verify that the technology in use meets the specified requirements.

4. Validate that the implemented system has met the required assurance level. The final validation confirms that the system achieves the required assurance level for the user-to-agency process. NIST SP 800-53A, *Guide for Assessing the Security Controls in*

Federal Information Systems and Organizations, Building Effective Security Assessment Plans, provides guidelines for the assessment of the implemented system during the validation process. Validation should be performed as part of a security authorization process that is described in NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*

5. Periodically reassess the information system to determine technology refresh requirements. Agencies should periodically reassess the information system to ensure that the identity authentication requirements continue to be satisfied. NIST SP 800-37, Rev 1, provides guidelines on the frequency, depth, and breadth of periodic reassessments. As with the initial validation process, agencies should follow the assessment guidelines specified in SP 800-53A for conducting the security assessment.

NIST Special Publication 800-63-1, *Electronic Authentication Guideline*

Written by William Burr, Donna Dodson, Elaine Newton, Ray Perlner, and Tim Polk of NIST, and by Sarbari Gupta and Emad Nabbus of Electrosoft, NIST SP 800-63-1 provides technical guidelines to agencies to allow individuals to remotely authenticate their identity to a federal information technology system.

SP 800-63-1 focuses on the implementation of Step 3 of the e-authentication process that was discussed in OMB Memorandum M-04-04. After completing a risk assessment and mapping the identified risks to the required assurance level, agencies can select appropriate technology that, at a minimum, meets the technical requirements for the required level of assurance.

The guideline presents an overview of the e-authentication process and provides details about the relationships and responsibilities of the participants involved in the process, including Registration Authorities (RAs), Verifiers, Relying Parties (RPs) and Credential Service Providers (CSPs), discussed below. Technical requirements are specified for each of the four levels of assurance as defined by OMB in the following areas:

· Identity proofing and registration of Applicants;

· Tokens (typically a cryptographic key or password) for authentication;

· Token and credential management mechanisms used to establish and maintain token and credential information;

· Protocols used to support the authentication mechanism between the Claimant and the Verifier; and

· Assertion mechanisms used to communicate the results of a remote authentication if these results are sent to other parties.

The techniques described in the guideline apply to traditional, widely implemented methods for remote authentication, based on secret information that the individuals to be authenticated prove that they know or possess.

NIST SP 800-63-1 includes definitions and abbreviations of the terms used in the publication, a list of references, and appendices that provide information on assessing the strength of passwords and on mapping Federal Public Key Infrastructure (PKI) certificate policies to e-authentication assurance levels. The guideline is available here.

E-Authentication Process

NIST SP 800-63-1 discusses the roles of individuals and organizations in the e-authentication process:

• The Applicant applies to a Registration Authority (RA) to become a Subscriber of a Credential Service Provider (CSP).
• If approved, the Subscriber is issued a credential by the CSP binding a token that contains a secret to be used in authentication processes to an identifier that the RA has verified.
• The individual whose identity is to be verified is the Claimant. Tokens are possessed by the Claimant, and are controlled through one or more traditional authentication factors (something you know, have, or are). The token may be issued by the CSP, generated directly by the Subscriber, or provided by a third party.
• Following registration, identity proofing and issuance, credentials and tokens are managed throughout their life cycle by the CSP.
• The authentication process establishes the identity of the Claimant to the Verifier who validates the Claimant's identity and the credentials that link the Claimant's token and identity.
• Assertion-based authentication employs statements from a Verifier to the Relying Party (RP) that contain information about a Subscriber, and is used when the RP and the Verifier are connected through a shared network. The RP uses the information in the assertion to identify the Claimant and make authorization decisions about access to resources controlled by the RP.

Technical Requirements for Four Levels of Assurance

The technical requirements for each of the four levels of assurance are:

• **Level 1** has no requirements for identity proofing, but the authentication mechanism used should provide some assurance that the same Claimant who participated in previous transactions is accessing the protected transaction or data. Level 1 allows for a wide range of available authentication technologies to be employed and permits the use of any of the token methods that are recommended for Levels 2, 3, or 4. Successful authentication requires that the Claimant prove through a secure authentication protocol that he or she possesses and controls the token.

Plaintext passwords or secrets are not transmitted across a network at Level 1. However, this level does not require cryptographic methods that block offline attacks by eavesdroppers. 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 Level 1, long-term shared authentication secrets may be revealed to Verifiers. Also at this level, assertions and assertion references require protection from manufacture/modification and reuse attacks.

• **Level 2** provides for single-factor remote network authentication. Identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. For single-factor authentication, Memorized Secret Tokens, Pre-Registered Knowledge Tokens, Look-up Secret Tokens, Out-of-Band Tokens, and Single-Factor One-Time Password Devices are allowed. Level 2 also permits any of the token methods that are recommended for Levels 3 or 4. Successful authentication requires that the Claimant prove through a secure authentication protocol that he or she controls the token. The controls applied at this level reduce the risks of online guessing, replay, session hijacking, and eavesdropping attacks. The protocols that are implemented are also required to provide some resistance to man-in-the middle attacks.

Long-term shared authentication secrets, if used, are never revealed to any other party except Verifiers operated by the Credential Service Provider (CSP); however, session, or temporary, shared secrets may be provided to independent Verifiers by the CSP. In addition to Level 1 requirements, assertions should be resistant to disclosure, redirection, capture, and substitution attacks. Approved cryptographic techniques are required for all assertion protocols used at Level 2 and above.

• **Level 3** provides for multi-factor remote network authentication. At least two authentication factors are required. At this level, identity-proofing procedures require verification of identifying materials and information. Authentication at Level 3 is based on proof of possession of the allowed types of tokens through a cryptographic protocol. Multi-factor Software Cryptographic Tokens are allowed at Level 3. Level 3 also permits any of the token methods that are allowed at Level 4. Authentication at Level 3 requires cryptographic strength mechanisms that protect the primary authentication token against compromise by the protocol threats for all threats at Level 2, as well as verifier impersonation attacks. Various types of tokens may be used, as described in NIST SP 800-63-1.

Authentication requires that the Claimant prove, through a secure authentication protocol, that he or she controls the token. The Claimant unlocks the token with a password or biometric, or uses a secure multi-token authentication protocol to establish two-factor authentication (through proof of possession of a physical or software token in combination with some memorized secret knowledge). Long-term shared authentication secrets, if used, are never revealed to any party except the Claimant and Verifiers

operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent Verifiers by the CSP. In addition to Level 2 requirements, assertions are protected against repudiation by the Verifier at Level 3.

• **Level 4** is intended to provide the highest practical remote network authentication assurance. Authentication at Level 4 is based on proof of possession of a key through a cryptographic protocol. At this level, in-person identity proofing is required. Level 4 is similar to Level 3 except that only "hard" cryptographic tokens are allowed. The token is required to be a hardware cryptographic module that has been validated for conformance with Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules,* Level 2 requirements, or higher overall with at least FIPS 140-2 Level 3 requirements for physical security. Level 4 token requirements can be met by using a Personal Identity Verification (PIV) Card with a PIV authentication key that is in compliance with FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors.*

Level 4 requires strong cryptographic authentication of all communicating 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. All protocol threats at Level 3 must be prevented at Level 4. Protocols shall also be strongly resistant to man-in-the-middle attacks. Long-term shared authentication secrets, if used, are never revealed to any party except the Claimant and Verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent Verifiers by the CSP. Approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated, using keys bound to the authentication process.

At Level 4, "bearer" assertions (assertions that do not provide a mechanism for the Subscriber to prove that he or she is the rightful owner of the assertion) are not used to establish the identity of the Claimant to the Relying Party (RP). "Holder-of-key" assertions may be used, provided that the assertion contains a reference to a key that is possessed by the Subscriber and is cryptographically linked to the Level 4 token used to authenticate to the Verifier. The RP should maintain records of the assertions it receives in order to support the detection of a compromised verifier impersonating the subscriber.

For More Information

NIST SP 800-63-1 provides many references to publications, regulations, and policies related to e-authentication, including:

Office of Management and Budget (OMB) Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, available here.

Agencies may determine based on their risk analyses that they need additional measures and safeguards to address privacy requirements and legal risks, for example. The following references provide information and guidance:

OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,* available here.

Department of Justice, *Guide to Federal Agencies: Legal Considerations in Designing and Implementing Electronic Processes,* available here.

General Services Administration (GSA), *Use of Electronic Signatures in Federal Organization Transactions*, see here.

In addition to the NIST publications referenced in this bulletin, other security-related publications are available on the NIST website to help organizations develop a comprehensive approach for determining the appropriate level of e-authentication assurance that they need and to select the best available technical solutions. See NIST's website here.

Information about NIST's information security programs is available from the Computer Security Resource Center here.