Multi-factor Authentication Implementation

Introduction

IRS Publication 1075, *Tax Information Security Guidelines for Federal, State, and Local Agencies* (Pub 1075) requires that all access to federal tax information (FTI) occurs from agency-owned equipment. It also requires that any remote access has multi-factor authentication implemented. Remote access, defined by Pub 1075, is any access to an agency information system by a user communicating through an external network (i.e. the internet). These requirements are more important as agencies, looking to reduce costs, allow employees to work from home or telework.

Multi-factor authentication drastically reduces the risk of identity theft and unauthorized disclosure of FTI. Multi-factor authentication decreases the probability that the requestor is not the person who he says he or she is. The number of factors is important, as it implies a higher probability that presenter of the identify evidence is who they claim to be.

This document explains the different authentication factors and addresses the security requirements for implementing multi-factor authentication to meet the requirements of the Office of Safeguards.

Mandatory Requirements

This message discusses detailed requirements that must be applied when procuring or developing various multi-factor authentication implementations. An agency may choose to implement a system appropriate to its needs, but all requirements contained in this memorandum that pertain to that implementation must be fulfilled.

Multi-factor authentication is required for “all remote network access to privileged and non-privileged accounts for information systems that receive, process, store or transmit FTI” (Pub 1075, *Section 9.3.7.2, Identification and Authentication (Organizational Users) (IA-2)*). This access requires the use at least two of the following types of authentication:

- **Something you know:** password, Personal Identification Number (PIN), challenge question, or pattern.
- **Something you have:** hardware or software token. Possession factors have been used for authentication for centuries, in the form of a key to a lock. The basic principle is that the key embodies a secret which is shared between the lock and the key, and the same principle underlies possession-factor authentication in computer systems. More information is provided below for implementation guidance. Federal Information Processing Standards (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, guidelines the standard for secure and reliable forms of identification.
• **Something you are**: biometric data. Biometric data may be verified in the form of a fingerprint, voiceprint or iris scan, using provided hardware and then entering a PIN or password in order to open the credential vault.

One type of authentication may not be repeated in attempting to satisfy multi-factor authentication. For example, authenticating using two passwords does not constitute multi-factor; they are both examples of “something you know” and can both only satisfy this category.

Multi-factor authentication is also required when accessing firewalls over an in-band connection, to provide an appropriate level of assurance of the identity of the individual configuring the device.

As a new requirement, if selecting an implementation that uses a personal identification number (PIN) (e.g., for activation of a token), the PIN must meet the following requirements:

- Minimum length of 8 digits,
- Have no repeating digit patterns (e.g., 55555555 or 3434343434)
- Disallow sequential digit strings (e.g., 12345678 or 98765432) and
- Not be stored with the hardware token.

**Something You Know**

Examples of this type of authentication are passwords or passphrases, usually employed with a username, PINs created and known by the user, for use with challenge questions, or patterns, such as a sequence on a keypad.

To be considered an appropriate authentication method, passwords must meet the requirements identified in Pub 1075, Section 9.3.7.5, *Authenticator Management (IA-5)*, which includes a minimum of eight characters, and a mixture of at least one numeric, one special character, one uppercase and one lowercase letter.

**Something You Have**

The most common examples of this authentication type are hardware and software tokens, such as the RSA SecurID fob or a smart card, that generate a random number sequence, or contain an embedded code, to be used by the user during the authentication process.

**Tokens**

Tokens are used by claimants to prove their identity and authenticate to a system or application, and can be either **software** or **hardware** based.

The token contains a secret that is used to prove the claimant is in control of the token. Token secrets are either based on asymmetric keys or symmetric (single) keys.
• In an asymmetric key model, the private key is stored on the token and used to prove possession when paired with the public key.
• Symmetric keys are shared directly between the claimant and the replying party for direct comparison over a secure channel (e.g. HTTPS).

Token input data, such as a challenge or nonce (number or bit string used only once), may be required to generate the token authenticator. Token input data may be supplied by the user or be a feature of the token itself (e.g. the clock in a One Time Password (OTP) device). Token activation data, such as a PIN may be required to activate the token and permit generation of an authenticator.

Soft Token Implementation

Software tokens are stored on a general-purpose computer such as a desktop, laptop or mobile device; and require activation through a second factor of authentication (e.g., PIN, password or biometric). Soft tokens are generally cheaper to implement and easier to manage than hard tokens, and avoid some physical security risks that come with hard tokens. However, soft tokens are only as secure as the computer they are stored on, and are susceptible to computer viruses, man-in-the-middle, phishing and other software attacks.

For remote access using multi-factor authentication, soft tokens are acceptable for the “something you have” factor with the following requirements implemented to protect the soft token software and the soft tokens for use with remote network authentication for access to FTI.

• **Private keys must be non-exportable** – Soft token software that utilizes encryption keys stored in a local key repository must mark the keys non-exportable. This helps prevent exportation of the key to be installed on an unauthorized system. Files of long-term private keys shall be protected by access controls that limit access to administrators and only to those applications that require access.
• **Never store keys in plain text (unencrypted) form** – If the soft token is using shared secret keys, the keys should not be stored in a format that can be read and copied outside of the application. Text files would have to be at least read only to the users of a system for the Soft Token software to function. This greatly increases the chance the keys can be copied to another system.
• **Distributing the seed record and initial passphrases requires a confidential channel to ensure that it is not duplicated in transit** – Installation of soft token software typically has two pieces of information (seed record, passphrase) to install and initialize the token generation engine. These two pieces of information, if captured by an unauthorized user would allow unauthorized installations of the software, and could be used by parties other than the authorized user.
• **Activation of the token must occur every time user authenticates using the soft token software** – Each authentication shall require entry of the password or other activation data. Input of the other factor (password) must be strictly limited to manual user input when challenged by the relying party (system). Storing of the PIN or password allowing the software to generate a token without manual user input should not be implemented.

• **Token time limit must be 2 minutes or less** – The token generated by the software must have a time limit for use. This small time window should be sufficient to initiate remote access, and prevents the sharing of a token for other systems, or theft of the token.

• **Soft token software password must follow Pub 1075 password requirements** – Password management requirements for soft token software should follow the complexity, size, change interval and reuse guidelines stated in Pub 1075. This will ensure that passwords used to generate tokens are not easily guessed and unique per user.

• **Audit all access to software tokens** – Audit logs must be captured for access to the soft token software when successful and unsuccessful remote access attempts have occurred. The audit trail should log attempts made to guess PIN numbers and passwords, and correlating software access with successful and unsuccessful remote access connections can show attempts to tamper or copy the soft token software.

• **Always install the latest version of malware prevention software before using Software Tokens** – Malware prevention software must be installed to identify and prevent installation of key logging software or other malware that could capture the PIN or password used to access the soft token software.

• **Always use FIPS 140-2 validated cryptographic modules** – The cryptographic module performing the encryption function must be validated to meet FIPS 140-2 Level 1.

Additionally, the IRS Office of Safeguards recommends agencies implement the following security controls. However, although these recommendations will decrease the likelihood that soft token software can be compromised, they are not required for Pub 1075 compliance.

• **PKI is the preferred key management platform** – Public-key infrastructure (PKI) uses asymmetric (public/private) key pairs for all cryptographic operations. With PKI, the claimant can prove itself to the system without disclosing the private keys. Symmetric keys must be disclosed to authenticate, so are more susceptible to compromise over time.

• **Use available Trusted Platform Modules (TPM)** – A TPM is a local hardware encryption engine and uses secured storage for encryption keys. By storing the keys in the TPM key store, direct access to the key is interrupted by the TPM system asking for authentication to access keys.
• **Perform self-validation before issuing a token** – Comparison of the software files, including the executable DLL and INI files against a hash or any other mechanism that validates the software has not been altered, must be performed before a token is given for remote access.

**Hard Token Implementation**

Hard tokens are physical tokens that store credentials on hardened, dedicated devices used to authenticate an identity. Hard tokens are susceptible to physical security attacks (i.e., direct physical access) if lost or stolen.

For multi-factor authentication, the following types of hard tokens are acceptable for the “something you have” authentication type. Each token has associated implementation requirements for use with remote network authentication for access to FTI.

• **Look Up Secret Token** – A physical token that stores a set of secrets, and is used to look-up the secret based on a prompt from the authentication protocol. An example of this is a grid-card.

• **Out of Band Token** – A one-time use token received over a separate channel from the primary authentication channel, and presented to the authentication protocol using the primary channel. An example of this is receiving a SMS message to a cell phone.

• **One-Time Password Device** – A hardware device that generates a one-time use passwords (e.g., sequence based or time based). The one-time password is typically displayed on the device and manually input to the authentication protocol, and may be activated by either “something you know” or “something you are.” Examples of this are tokens that generate a code every 30-60 seconds, or has a button that when pressed, generates a code. This could also include a one-time password generating application running on a cell phone or mobile device. The cryptographic module performing the verifier function shall be FIPS 140-2 validated, and the one-time password must be generated by using an FIPS-approved block cipher or hash function to combine a symmetric key stored on a personal hardware device with a nonce. The one-time password shall have a limited lifetime.

• **Cryptographic Device** - A hardware device that contains non-programmable logic and non-volatile storage dedicated to all cryptographic operations and protection of private keys. An example of this is a FIPS-201 smart card that contains several X.509 certificates and all processing of cryptographic functions. Each authentication requires entry of the activation data (e.g., password, PIN).

In addition, shared secret files shall also be encrypted so that the encryption key for the shared secret file is encrypted under a key held in a FIPS 140-2 validated hardware cryptographic module.

**Something You Are**
Biometric authentication also satisfies the regulatory definition of multi-factor authentication. Users may biometrically authenticate via fingerprint, voiceprint or iris scans using provided hardware, and typically in combination with a password.

**Example Implementations**

As previously described, the basic requirement for systems that handle FTI is that two of the three types of authentication methods (see mandatory requirements at the beginning of this document) must be used to meet compliance requirements.

A username and password at the network boundary, with an additional, distinct username and password at the application would not meet these requirements. While the user is presenting two separate credentials, they are both something the user knows.

Many agencies have implemented a “phone factor” type of implementation, where a user identifies a phone number that the user will have possession of – typically a mobile phone. The user logs into a system with a username and password. This triggers the remote access system to contact the user by means of the phone, asking the user to confirm the attempt to begin a remote session by pressing a key.

This implementation does not confirm that the intended user does actually possess the phone, however; any individual with access to that phone could press a key. This can be corrected by using the phone, either by text message or voice call, to provide the user with a code to enter into the primary authentication channel.

**Resources**

Additional information can be found in the following documents:

- FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*  