PCI Security Standards Council

INFORMATION SUPPLEMENT

Multi-Factor Authentication

Version: 1.0
Date: February 2017
Author: PCI Security Standards Council

Table of Contents

Overview

The intent of multi-factor authentication (MFA) is to provide a higher degree of assurance of the identity of the individual attempting to access a resource, such as physical location, computing device, network or a database. MFA creates a multi-layered mechanism that an unauthorized user would have to defeat in order to gain access.

This document describes the industry-accepted principles and best practices associated with multi-factor authentication. The guidance in this document is intended for any organization evaluating, implementing, or upgrading a MFA solution, as well as providers of MFA solutions.

MFA and PCI DSS

PCI DSS requires MFA to be implemented as defined in Requirement 8.3 and its sub-requirements[1]. Guidance on the intent of these requirements is provided in the Guidance column of the standard, which includes; *"Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication (as described in Requirement 8.2), before access is granted."* The additional guidance in this document does not extend the PCI DSS requirement beyond what is stated in the standard.

While PCI DSS Requirement 8.3 does not currently require organizations to validate their MFA implementation to all the principles described in this guidance document, these principles may be incorporated in a future revision of the standard. Organizations are therefore strongly encouraged to evaluate all new and current MFA implementations for conformance to these principles.

Terminology

In addition to terms defined in the *PCI DSS Glossary of Terms, Abbreviations, and Acronyms*, the following acronyms are referenced:

Term	Description
SE	Acronym for Secure Element. Tamper-resistant hardware platform, capable of securely hosting applications and storing confidential and cryptographic data.
TEE	Acronym for Trusted Execution Environment. Software that provides security features such as isolated execution.
TPM	Acronym for Trusted Platform Module. Module that is dedicated and physically isolated from the rest of the processing system microcontroller, which is designed to secure hardware by integrating cryptographic keys into devices. It offers facilities for the secure generation of cryptographic keys and limitation of their use.

[1] Refers to PCI DSS v3.2

Authentication Factors

The overall authentication process for MFA requires at least two of the three authentication methods described in PCI DSS Requirement 8.2:

a) **Something you know,** such as a password or passphrase. This method involves verification of information that a user provides, such as a password/passphrase, PIN, or the answers to secret questions (challenge-response).

b) **Something you have,** such as a token device or smartcard. This method involves verification of a specific item a user has in their possession, such as a physical or logical security token, a one-time password (OTP) token, a key fob, an employee access card, or a phone's SIM card. For mobile authentication, a smartphone often provides the possession factor in conjunction with an OTP app or a cryptographic material (i.e., certificate or a key) residing on the device.

c) **Something you are,** such as a biometric. This method involves verification of characteristics inherent to the individual, such as via retina scans, iris scans, fingerprint scans, finger vein scans, facial recognition, voice recognition, hand geometry, and even earlobe geometry.

Other types of information, such as geolocation and time, may be additionally included in the authentication process; however, at least two of the three factors identified above must always be used. For example, geolocation and time data may be used to restrict remote access to an entity's network in accordance with an individual's work schedule. While the use of these additional criteria may further reduce the risk of account hijacking or malicious activity, the remote access method must still require authentication via at least two of the following factors: something you know, something you have, and something you are.

Independence of Authentication Mechanisms

The authentication mechanisms used for MFA should be independent of one another such that access to one factor does not grant access to any other factor, and the compromise of any one factor does not affect the integrity or confidentiality of any other factor. For example, if the same set of credentials (e.g., username/password) is used as an authentication factor and also for gaining access to an e-mail account where a secondary factor (e.g., one-time password) is sent, these factors are not independent. Similarly, a software certificate stored on a laptop (something you have) that is protected by the same set of credentials used to log in to the laptop (something you know) may not provide independence.

The issue with authentication credentials embedded into the device is a potential loss of independence between factors—i.e., physical possession of the device can grant access to a secret (something you know) as well as a token (something you have) such as the device itself, or a certificate or software token stored or generated on the device. As such, independence of authentication factors is often accomplished through physical separation of the factors; however, highly robust and isolated execution environments (such as a Trusted Execution Environment [TEE], Secure Element [SE], and Trusted Platform Module [TPM]) may also be able to meet the independence requirements.

Out-of-Band Authentication

Out-of-band (OOB) refers to authentication processes where authentication methods are conveyed through different networks or channels.

Where authentication factors are conveyed through a single device/channel—for example, entering credentials via a device that also receives, stores, or generates a software token—a malicious user who has established control of the device has the ability to capture both authentication factors.

Transmission of a one-time password (OTP) to a smartphone has traditionally been considered an effective out-of-band method. However, if the same phone is then used to submit the OTP—for example, via a web browser—the effectiveness of the OTP as a secondary factor is effectively nullified.

Out-of-band conveyance of authentication mechanisms is an additional control that can enhance the level of assurance for multi-factor authentication. In lieu of the ability to use out-of-band communication, the authentication process should establish controls to guarantee that the individual attempting to use the authentication is, in fact, the legitimate user in possession of the authentication factor.

Cryptographic Tokens

Cryptographic tokens may be embedded into a device or stored on separate, removable media. The following guidance is based on NIST SP800-164[2] and NIST SP800-157[3], and considers some common form factors that are often used with mobile computing devices.

[2] NIST Special Publication 800-164 (Draft), *Guidelines on Hardware-Rooted Security in Mobile Devices (Draft).* URL: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf (accessed: November 07, 2016).

[3] NIST Special Publication 800-157 *Guidelines for Derived PIV Credentials.* URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf (accessed: November 07, 2016)

Removable (Non-Embedded) Hardware Cryptographic Tokens

In this category of devices, a private key resides in a hardware cryptographic module (or physical security token) that is physically separate from the mobile computing device. Access to either the mobile computing device or cryptogram stored on the token does not grant access to the other, thus maintaining the independence of authentication factors.

Each of the form factors described below supports a secure element (SE), a tamper-resistant cryptographic component that provides security and confidentiality in mobile devices.

- **SD Card with Cryptographic Module** – A non-volatile memory card format for use in portable devices such as mobile phones and tablet computers.
- **Removable UICC with Cryptographic Module** – The Universal Integrated Circuit Card (UICC) configuration is based on the GlobalPlatform Card Specification v2.2.1 [GP-SPEC] and provides storage and processing, as well as input/output capabilities.
- **USB Token with Cryptographic Module** – A Universal Serial Bus (USB) token is a device that plugs into the USB port on various IT computing platforms, including mobile devices and personal computers. USB tokens typically include onboard storage and may also include cryptographic processing capabilities—e.g., cryptographic mechanisms to verify the identity of users. USB token implementations that contain an integrated secure element (an integrated circuit card or ICC) are suitable for use in the authentication process.

Embedded Cryptographic Tokens

An authentication credential and its associated private key may be used in cryptographic modules that are embedded within mobile devices[4]. These modules may either be in the form of a hardware cryptographic module that is a component of the mobile device or in the form of a software cryptographic module that runs on the device.

Hardware cryptographic modules are preferred over software due to their immutability, smaller attack surfaces, and more reliable behavior; as such, they can provide a higher degree of assurance that they can be relied upon to perform their trusted function or functions.

Protecting and using the authentication credential and the corresponding private key in software may potentially increase the risk that the key could be stolen or compromised.

[4] Draft NIST Interagency Report 7981, Mobile, PIV, and Authentication. URL: http://csrc.nist.gov/publications/drafts/nistir-7981/nistir7981_draft.pdf (accessed: November 07, 2016)

Protection of Authentication Factors

To prevent misuse, the integrity of the authentication mechanisms and confidentiality of the authentication data need to be protected. The controls defined in PCI DSS Requirement 8 provide assurance that authentication data is protected from unauthorized access and use. For example:

- Passwords and other "something you know" data should be difficult to guess or brute-force, and be protected from disclosure to unauthorized parties.
- Biometrics and other "something you are" data should be protected from unauthorized replication or use by others with access to the device on which the data is present.
- Smart cards, software certificates, and other "something you have" data should not be shared, and should be protected from replication or possession by unauthorized parties.

Where any authentication elements rely on a multi-purpose consumer device—e.g., mobile phones and tablets—controls should also be in place to mitigate the risk of the device being compromised.

Multi-step vs. Multi-Factor

PCI DSS requires that all factors in multi-factor authentication be verified prior to the authentication mechanism granting the requested access. Moreover, no prior knowledge of the success or failure of any factor should be provided to the individual until all factors have been presented. If an unauthorized user can deduce the validity of any individual authentication factor, the overall authentication process becomes a collection of subsequent, single-factor authentication steps, even if a different factor is used for each step. For example, if an individual submits credentials (e.g., username/password) that, once successfully validated, lead to the presentation of the second factor for validation (e.g., biometric), this would be considered "multi-step" authentication.

It is possible for both multi-step and multi-factor authentication to be present in an environment. For example, an individual may perform an authentication step in order to log in to a computer before initiating a separate MFA process to gain access to the CDE. An example of this scenario would be a remote user entering credentials to log in to their corporate laptop. The user may then initiate a VPN connection to the organization's network using a combination of credentials and a physical smartcard or hardware token.

Use of SMS for Authentication

PCI DSS relies on industry standards—such as NIST, ISO, and ANSI—that cover all industries, not just the payments industry. While NIST currently permits the use of SMS, they have advised that out-of-band authentication using SMS or voice has been deprecated and may be removed from future releases of their publication[5].

Laws and Regulations

Organizations need to be aware of local and regional laws that may also define requirements for the use of MFA. For example, there may be additional requirements around consumer authentication used to initiate payments or to conduct high-risk transactions, such as the European Union Directive on Payment Services (PSD2) and the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook. Additionally, some laws or regulations may have more stringent MFA requirements than those required by PCI DSS.

PCI SSC encourages all organizations to be aware of the potential impact that local laws and regulations may have on their MFA implementations. PCI DSS requirements for multi-factor authentication do not supersede local or regional laws, government regulations, or other legal requirements.

[5] DRAFT NIST Special Publication 800-63B Digital Authentication Guideline. URL: https://pages.nist.gov/800-63-3/sp800-63b.html (accessed: November 07, 2016)

Common Authentication Scenarios

This section explores some common authentication scenarios and considerations for multi-factor authentication.

Scenario 1

An individual uses one set of credentials (password A) to log in to a device and also to access a software token stored on the device. The individual then establishes a connection to the CDE/corporate network, providing a different set of credentials (password B) and the OTP generated by the software token as authentication.

The authentication system grants the requested access if both factors provided are valid:

- Something you know – Password B
- Something you have – Software token

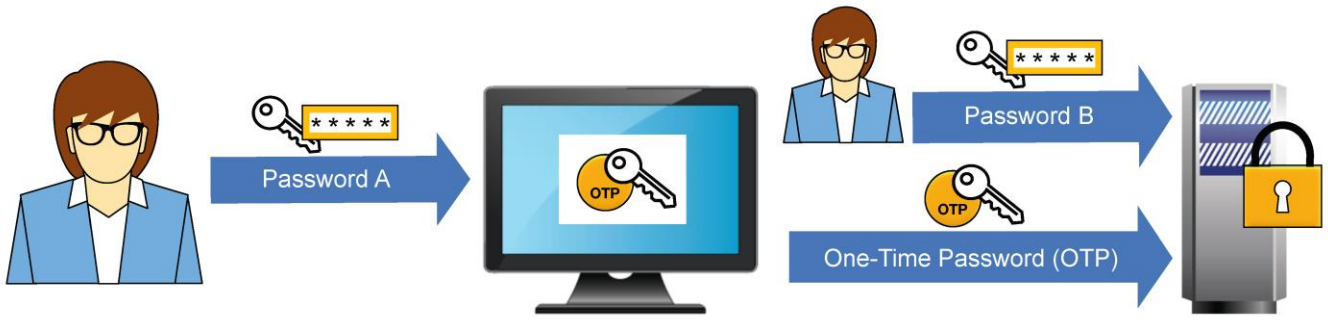

Figure 1: Scenario 1

To ensure the independence of authentication factors is maintained, this scenario requires that the software token ("something you have") is embedded into the physical device in such way that it cannot be copied or used on any other device.

Furthermore, physical security over the device becomes a required security control as proof of possession of the device. Otherwise, if access to software token is merely a reflection of the ability to login into the device (either locally or remotely), the overall authentication process is a usage of "something you know" twice.

Scenario 2

In this scenario, the individual uses one set of credentials (e.g., username/password or biometric) to log in to the device; and those credentials also provide access to a software token stored on the device. To initiate a connection to the CDE/corporate network, the user launches a browser window that pre-populates a different set of credentials (e.g., cached on the device or using password manager) in conjunction with the software token.

Figure 2: Scenario 2

This scenario does not provide independence between authentication factors, as a single set of credentials (Password A) provides access to both factors (password B and software token).

Scenario 3

In this scenario, the individual uses one set of credentials (e.g., username/password) to log in into the computer. The connection to the CDE/corporate network requires both the initial set of credentials and an OTP generated by a software token residing on a mobile device.

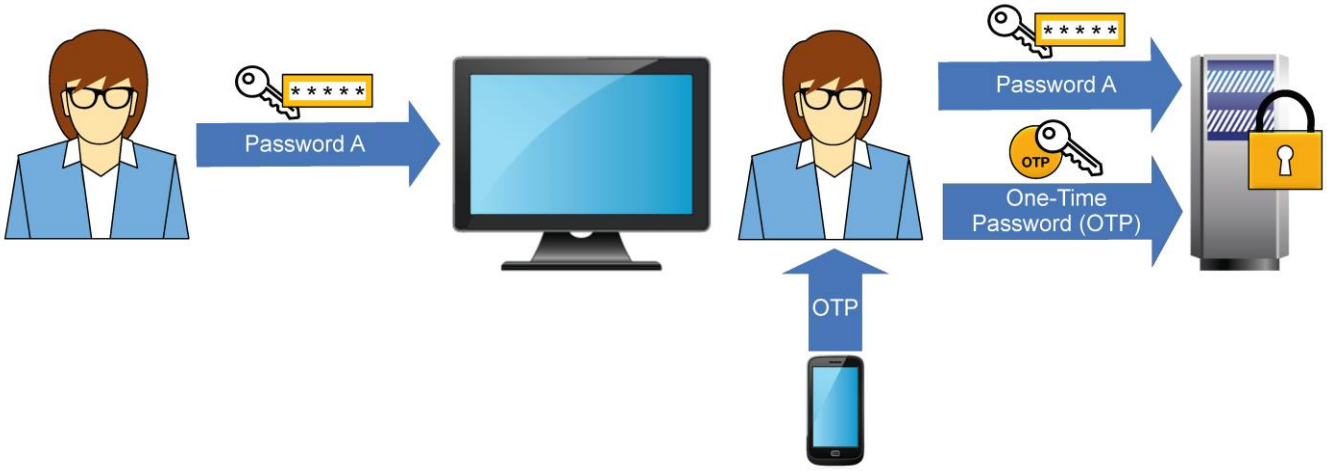

Figure 3: Scenario 3

Even though the individual uses the same password (something you know) to authenticate both to the laptop and the CDE/corporate network, the software token residing on a mobile phone provides a second (something you have) factor that maintains independence between authentication mechanisms.

If the mobile device is also used to initiate the connection to the CDE/corporate network, additional security controls would be needed to demonstrate independence of the authentication mechanisms.

Scenario 4

In this scenario, the individual uses multi-factor authentication (e.g., password and biometric) to log in to a smartphone or a laptop. To establish a non-console connection to the CDE/corporate network, the individual then provides a single authentication factor (e.g., a different password, digital certificate, or signed challenge-response).

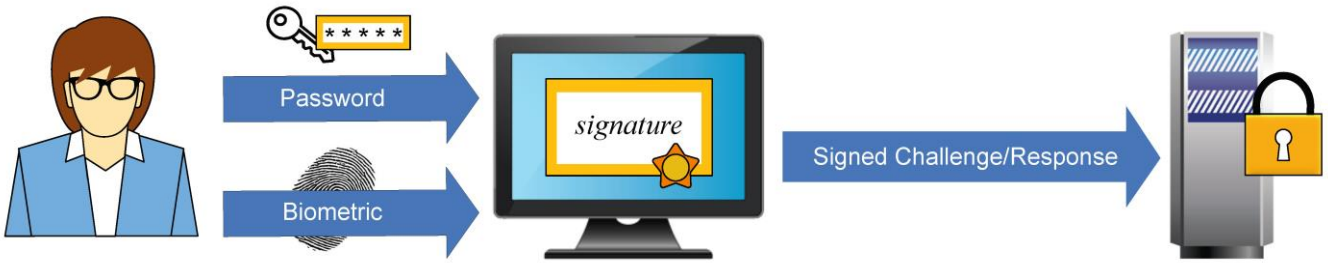

Figure 4: Scenario 4

In this scenario, the device (smartphone or laptop) should be hardened and controlled to guarantee that the multi-factor authentication is properly implemented and always performed before initiating the connection to the CDE/corporate network. This includes ensuring that users cannot change or disable security configurations—e.g., to disable or bypass multi-factor authentication—and that independence of authentication factors is maintained.

Moreover, additional controls may be needed to prevent an unauthorized party from gaining constructive use of the "trust" established between the device and the CDE/corporate network. An example of constructive use would be for a malicious user to execute a process on the device that allows them to interact with the CDE/corporate network, without having knowledge of the password or biometric used by the legitimate user.

Where the user manages their own device—e.g., in a BYOD environment—the user-managed device should maintain a robust and isolated execution environment (such as TEE, SE, or TPM) that cannot be adversely impacted or bypassed by the user. Otherwise, the organization would have no assurance that MFA is properly implemented and enforced on the device.