



QMan SMS Hero

SMS Auth Codes and Industry Security Standards Compliances

The Requirements

If your company is working on getting or staying PCI or HIPAA compliant let QMan SMS Hero's tool, SMS Auth Codes, help. Two-factor authentication (2FA), also referred to as multi-factor authentication (MFA), is typically one aspect of these and other industry security standards. For PCI, [PCI DSS v3.2 Requirement 8.3](#) specifies that an implementation of a 2FA mechanism must meet the following two requirements:

1. Your overall authentication process requires that a user must authenticate through at least *two of the three* following authentication methods:
 - a. Something the user knows.
 - b. Something the user has.
 - c. Something the user is.
2. The two authentication mechanisms used are independent of one another.

The above definition of 2FA was not invented specifically for PCI. It is actually the de facto standard definition of 2FA/MFA and many industry security standards have adopted this definition. You should check the documented security standards that you are interested in first, but chance are, if you implement 2FA that adheres to this definition, you should be good to go.

Getting Two Out Of Three

First let's take a look at requirement one, which requires the two of three authentication methods are used.

The authentication method for item 1c, something the user is, really refers to biometric authentication. These are such things as reading from a finger print reader or a full hand scanner. Biometric authentication is usually found at places such as data center entrances or other secure physical sites. This is typically not where QMan SMS Auth Codes is being used so we will ignore item 1c and focus our attention on 1a and 1b.

Item 1a, something the user knows, we are very familiar with and that is passwords and answers to security questions.

Item 1b, something the user has, is where QMan SMS Auth Codes come in to play. When QMan SMS Auth Codes sends an authorization code to a smartphone, the user has been given something for one-time use and that meets the criteria for item 1b. Challenging the user to input a password and a QMan SMS auth code provides the two out of three authentication methods required by PCI and other security standards.

Additionally, a user inputting a password into a login page of a portal and the smartphone in the user's hand with a QMan SMS auth code on it are also independent of each other and therefore also meets the above item 2 requirement for 2FA.

Multi-Factor vs. Multi-Step

If you are implementing 2FA or MFA for the purposes of gaining an industry security certification, you should also be aware of subtle but important distinction between multi-factor authentication and multi-step authentication. One of the keys to a proper 2FA process is that it is multi-factor and not multi-step.

So...what is the difference? Multi-factor is an authentication process where, if one of the factors fails authentication, the user does not know which one failed. Multi-step is where the user is told or could deduce which of the authentication methods failed.

Here is a simple example. For a customer portal, you could implement a true two-factor authentication process by implementing a login flow where the user is asked for only their user name on the first screen and must click an Ok button to go to screen two. Using the user name, the portal software looks up the user and, if found, issues a QMan SMS auth code to the user's SMS capable phone number of record. The user is then presented with screen two where they have to input both their password and the auth code that they were issued. When the user clicks the Ok button on screen two, if either the password or auth code is incorrect, the user is simply told that their login failed, but does not know which the two authentication methods were incorrect.

For a complete understanding of all the feature of QMan SMS Auth Codes, as well as an understanding of how all of the QMan SMS Hero tools work, click the Watch Demo button on the [QMan AppExchange](#) web page. If you have any questions, you can send an email to info@3creekstech.com.

