

Is phishing-resistant authentication alone acceptable as multi-factor authentication for PCI DSS Requirements 8.4.1 and 8.4.3?

PCI SSC FAQ | Article 1596 | May 2025

No, phishing-resistant authentication cannot be used without an additional authentication factor to meet Requirements 8.4.1 or 8.4.3 because of the increased risk with these types of access.

Use of phishing-resistant authentication is encouraged and recommended; however, to meet Requirements 8.4.1 and 8.4.3 for MFA, phishing-resistant authentication must be used with another factor (for example, a password, PIN, or biometric).

See also:

FAQ 1595: Are passkeys synced across devices, implemented according to the FIDO2 requirements, acceptable for use as phishing-resistant authentication to meet PCI DSS Requirement 8.4.2 (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/are-passkeys-synced-across-devices-implemented-according-to-the-fido2-requirements-acceptable-for-use-as-phishing-resistant-authentication-to-meet-pci-dss-requirement-8-4-2/)?

Source: <https://www.pcisecuritystandards.org/faqs/1596/>