

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?

PCI SSC FAQ | Article 1595 | May 2025

Yes. Passkeys synced across devices (also called synced passkeys), implemented according to the FIDO2 requirements, are considered phishing-resistant authentication, and may be used as a single authentication factor in place of multi-factor authentication (MFA) to meet PCI DSS Requirement 8.4.2. This aligns with the Applicability Note in Requirement 8.4.2. Passkeys not implemented according to the FIDO2 requirements must include an additional factor to meet PCI DSS Requirements 8.4.1, 8.4.2, and 8.4.3 for MFA.

See also:

FAQ 1596: Is phishing-resistant authentication alone acceptable as multi-factor authentication for PCI DSS Requirements 8.4.1 and 8.4.3 (https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/is-phishing-resistant-authentication-alone-acceptable-as-multi-factor-authentication-for-pci-dss-requirements-8-4-1-and-8-4-3/)?

Source: <https://www.pcisecuritystandards.org/faqs/1595/>