

Understanding the SAQs for PCI DSS version 3

The PCI DSS self-assessment questionnaires (SAQs) are validation tools intended to assist merchants and service providers report the results of their PCI DSS self-assessment. The different SAQ types are shown in the table below to help you identify which SAQ best applies to your organization. Detailed descriptions for each SAQ are provided within the applicable SAQ.

Note: Entities should ensure they meet all the requirements for a particular SAQ before using the SAQ. Merchants are encouraged to contact their merchant bank (acquirer) or the applicable payment brand(s) to identify the appropriate SAQ based on their eligibility.

SAQ	Description
A	Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS validated third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Not applicable to face-to-face channels.</i>
A-EP*	E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. <i>Applicable only to e-commerce channels.</i>
B	Merchants using only: <ul style="list-style-type: none"> • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
B-IP*	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. <i>Not applicable to e-commerce channels.</i>
D	<p>SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types.</p> <p>SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.</p>

* New for PCI DSS v3.0