

Is storage of encrypted cardholder data considered "cardholder data" per the SAQ eligibility criteria?

PCI SSC FAQ | Article 1314 | January 2015

Yes, encrypted cardholder data is considered cardholder data for the purposes of the SAQ eligibility criteria.

Merchants must meet all the defined eligibility criteria for a particular SAQ in order to use that SAQ. The eligibility criteria for all SAQs, except SAQ D, include an attestation by the merchant that they do not store cardholder data in electronic format. As SAQ D is the only SAQ that includes PCI DSS requirements for protecting stored cardholder data, including encryption and key management requirements, SAQ D could apply to scenarios where only encrypted cardholder data is stored.

Merchants should consult with their acquirer or the payment brands directly (as applicable) to determine which SAQ they should use. Contact details for the payment brands can be found in FAQ #1142 - How do I contact the payment card brands?

See also FAQ # 1086 Is encrypted cardholder data in scope for PCI DSS?

Source: <https://www.pcisecuritystandards.org/faqs/1314/>