

Are authentication values from a 3DS transaction considered sensitive authentication data for PCI DSS purposes?

PCI SSC FAQ | Article 1603 | March 2026

No. PCI DSS sensitive authentication data (SAD) consists of full magnetic-stripe data, card verification codes or values, and PINs or PIN blocks. PCI DSS specifically prohibits storage of SAD after completion of the authorization process.

The 3-D Secure (3DS) authentication value is a cryptographic value generated by the 3DS Access Control Server that allows the authorization system to validate the integrity of the authentication result during authorization processing. This 3DS value is also referred to as the cardholder authentication value (CAVV) and the accountholder authentication value (AAV). The authentication value is one of the data elements identified as 3DS sensitive data in the PCI 3DS Data Matrix in Table 1: 3DSS, DS, and ACS Sensitive Data Elements. Data elements included in this table are subject to the requirements in the PCI 3DS Core Security Standard that apply to 3DS sensitive data.

3DS authentication values and other 3DS sensitive data are not considered to be SAD from a PCI DSS perspective and PCI DSS does not prohibit 3DS sensitive data from being stored after the authorization process is complete.

Entities performing or providing any of the following 3DS functions: 3DS Server, 3DS Directory Server, and/or 3DS Access Control Server should confirm with the payment brand(s) for which they perform these 3DS functions whether they are required to meet the requirements in the PCI 3DS Core Security Standard.

Source: <https://www.pcisecuritystandards.org/faqs/1603/>