

# **How does PCI DSS Requirement 6.4.3 apply to 3DS scripts called from a merchant check-out page as part of 3DS processing?**

PCI SSC FAQ | Article 1581 | August 2024

---

The objective of PCI DSS Requirement 6.4.3 is to ensure that unauthorized code cannot be executed in the payment page as it is rendered in the consumer's browser.

In a typical 3DS implementation, 3DS Server fetches and stores URLs to scripts from an EMV 3DS Access Control Server (ACS), EMV 3DS Directory Server (DS), or services connected to the ACS or DS, on behalf of an issuer, issuer agent, or payment network. During the checkout process, a merchant website serves a web page with an iframe using a URL provided by the 3DS Server with an applicable script to support 3DS functionality.

For merchants using a 3DS solution, validation to PCI DSS Requirement 6.4.3 for 3DS scripts is not required due to the inherent trust relationship between the 3DS service provider and the merchant, as established in the merchant's due diligence and onboarding processes, and the business agreement between the entities.

Any script run outside of the purpose of performing a 3DS functionality is subject to PCI DSS requirement 6.4.3.

Source: <https://www.pcisecuritystandards.org/faqs/1581/>