

Why is SAQ A-EP used for Direct Post while SAQ A is used for iFrame or URL redirect?

PCI SSC FAQ | Article 1291 | August 2015

There is a distinct difference in terms of how payment data is accepted between Direct Post & iFrames/redirects, which is why there are different SAQs. In a Direct Post implementation, the merchant website produces some or all of the web page that is used to accept payment data, and then passes it directly to the third-party payment processor. In this implementation, the consumer (cardholder) never leaves the merchant website. Conversely, with a redirect or iFrame, the third-party payment processor produces the webpage that accepts payment data. The merchant website is not directly involved in the acceptance of payment data as this is directly accepted by the third-party payment processor. In these implementations, the consumer leaves the merchant website and goes to the payment processor for payment acceptance and processing.

This data flow is a key difference between the different methods, and is reflected in the eligibility criteria for SAQ A and SAQ A-EP as follows:

-

SAQ A: All elements of the payment page(s) delivered to the consumer's browser originate only and directly from a PCI DSS validated third-party service provider(s)

- SAQ A-EP: Each element of the payment page(s) delivered to the consumer's browser originates from either the merchant's website or a PCI DSS compliant service provider(s)

Source: <https://www.pcisecuritystandards.org/faqs/1291/>