sysnet global solutions

Ecommerce SAQ Selection

Ecommerce SAQ Selection: A Guide. Version 2.0, July 2017

Natasja Bolton, CISSP, QSA. Senior Acquirer Support QSA

Introduction

Determining which PCI DSS Self-Assessment Questionnaire (SAQ) is appropriate to a merchant's ecommerce web presence can be difficult.

Often merchants are advised by their web developer or payment solution provider to believe a particular SAQ is appropriate to their business but find, when they engage with their acquirer, that in fact a more complex and demanding SAQ assessment is required.

In this updated whitepaper, which takes into account PCI SSC guidance published since its initial release in November 2015, we provide a guide to help both merchants and their acquirers reach the same conclusions with regards to the appropriate ecommerce SAQ selection.

Available Ecommerce SAQs

There are only three SAQs that can apply to ecommerce websites:

SAQ A	All payment acceptance and processing are entirely outsourced to PCI DSS validated third party service providers, e.g. *Wholly outsourced ecommerce entirely provided/operated by a validated PCI DSS compliant Service Provider* OR *Redirect to a hosted payment page (or iFrame of same) provided by a validated PCI DSS compliant service provider)*
SAQ A-EP	All processing of cardholder data is outsourced to a PCI DSS validated third party payment processor but the merchant website does have an impact on how cardholder is accepted, e.g. *Merchant website presents the payment page but processing of the cardholder data is handled by a validated PCI DSS compliant Service Provider, such as a website configured for direct post to force submission of the cardholder data direct from the browser to the payment processor*
SAQ D	The merchant website is involved in both the acceptance and processing of the cardholder data, e.g. *Merchant website presents the payment page, accepts/captures the cardholder data and uses a method of direct integration (such as direct API) to submit that cardholder data to the payment processor*

Selecting the correct Ecommerce SAQ

The applicability and features of each SAQ is discussed in turn.

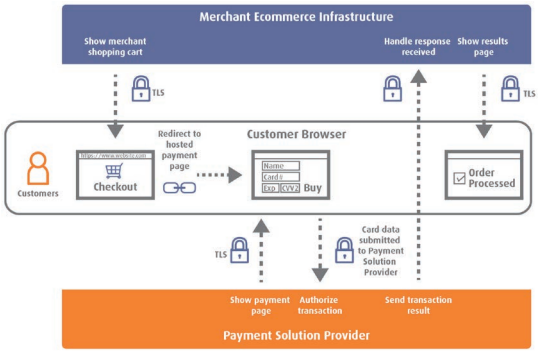
SAQ A

SAQ A applies to SAQ eligible ecommerce merchants where all payment acceptance and processing are entirely outsourced to a PCI DSS validated third party service provider(s).

This could be where:

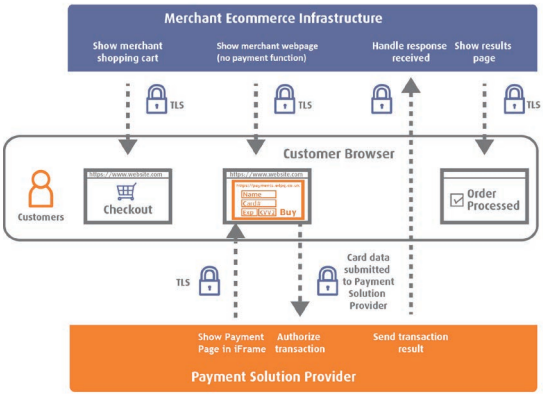
1. The merchant's website fully redirects (URL redirect) the customer browser to a **hosted payment page** that is delivered in its entirety from a PCI DSS validated third party service provider.
2. The merchant's website delivers the hosted payment page, sourced in its entirety from a PCI DSS validated third party service provider, embedded within an **iFrame** on their web page.
3. The merchant has **wholly outsourced** their ecommerce website and relies entirely on a validated PCI DSS compliant ecommerce solution provider for all aspects of their website and ecommerce development, maintenance and hosting (where that third party is validated for all applicable PCI DSS requirements given the scope of the services provided, which may include Appendix A)

The diagram below illustrates the **hosted payment page method**, showing how this method fulfils the criteria for SAQ A.



The payment page (the page requesting and capturing the payment card data) is delivered in its entirety from the Payment Solution Provider (PSP). All elements of the payment page are sourced/delivered directly from the validated PCI DSS compliant third party PSP.

The second diagram below shows the difference between the URL redirect method and the iFrame.



In this case the hosted payment page is embedded within an **iFrame** on the merchant's webpage but it is still the case that the entirety (all elements of) the payment page being delivered to the customer browser **originate only and directly** from the validated PCI DSS compliant PSP.

It is not always easy to tell whether the payment page that pops up is a hosted payment page. Often the URL is not immediately visible in the pop-up payment window that appears, such as this mock-up:

However, use of the web browser's developer tools may help to determine that the pop-up window is, as an example, a modal iFrame with a source URL (`src`) of the validated PCI DSS compliant PSP. In other words, the **entirety** of the payment page is still being delivered from the validated PCI DSS compliant PSP.

We have also seen instances where, on first inspection it looks like the ecommerce website uses an SAQ A-EP rather than an SAQ A eligible method: it appears that JavaScript is being used to create the payment page or that the merchant is *"embedding a payment form in a <DIV>*[1] *".* On further investigation, it may become apparent that the merchant page calls JavaScript to instantiate an iFrame with a source of the PSP's hosted payment page: e.g. `iframe src=https://PSP_hosted_payment_page`.

PCI SSC FAQ 1438 describes how to determine the payment page when using an iFrame and hence confirm the ecommerce implementation's SAQ A eligibility: "*Where the payment page is embedded within an iframe on a page on the merchant's website, all fields and web elements associated with capturing payment card data must be contained within the iframe* [originating only and directly from a PCI DSS validated third party service provider(s)] *to be eligible for SAQ A*".
PCI SSC FAQ 1438 describes how to determine the payment page when using an iFrame and hence confirm the ecommerce implementation's SAQ A eligibility: "*Where the payment page is embedded within an iframe on a page on the merchant's website, all fields and web elements*

1 Reference: http://pcissc.force.com/faq/articles/Frequently_Asked_Question/Why-is-there-a-different-approach-for-Direct-Post-implementations-than-for-iFrame-and-URL-redirect-what-are-the-technical-differences-and-how-do-they-impact-the-security-of-e-commerce-transactions

associated with capturing payment card data must be contained within the iframe [originating only and directly from a PCI DSS validated third party service provider(s)] to be eligible for SAQ A".

The **wholly outsourced ecommerce** implementation, Option 3. above, also fulfils the criteria for SAQ A because[2]:

- All processing of cardholder data is entirely outsourced to PCI DSS validated third party service providers
- All third party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant
- 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)

Therefore, if a validated ecommerce solution provider's PCI DSS compliance assessment encompassed all aspects of the hosting, development, maintenance and payment operations of their managed solution in its scope, then a wholly outsourced merchant ecommerce website may utilise the direct integration ecommerce method and still be eligible for SAQ A.

SAQ A-EP

SAQ A-EP applies to SAQ eligible ecommerce merchants where all processing of cardholder data is outsourced to a PCI DSS validated third party payment processor but the merchant website has an impact on how cardholder data is accepted.

SAQ A-EP applies to SAQ eligible merchants where:

- All processing of cardholder data, with the exception of the payment page, is outsourced to a PCI DSS validated third party payment processor,
- The merchant website does affect the security of the payment transaction and/or,
- The merchant website does affect the integrity of the page that accepts the consumer's cardholder data,
- The merchant website does not receive, process or transmit cardholder data.

NOTE: To be eligible for SAQ A-EP any third party hosting provider the merchant website relies upon must be validated for all applicable PCI DSS requirements.

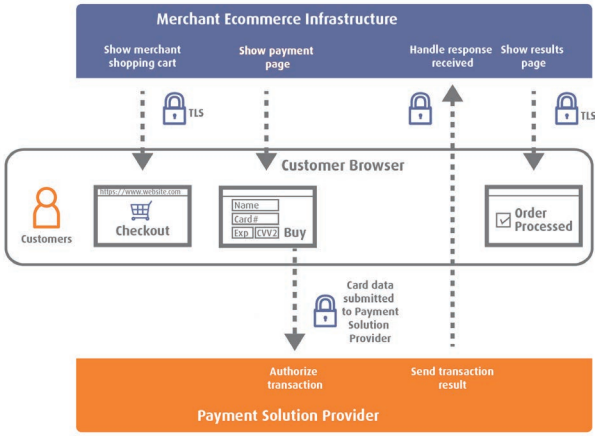
If a merchant website using an SAQ A-EP eligible integration method is hosted by a third party provider, the merchant must ensure that the third party is a validated PCI DSS compliant service provider (this may need to include PCI DSS Appendix A if the provider is a shared hosting provider).

This is because in a third party hosted scenario many of the PCI DSS requirements in SAQ A-EP are not within the merchant's ability to control. For example, the merchant may have no influence over firewall/network management (requirement 1) or of system configuration standards (requirement 2) or vulnerability/patch management (requirement 6), especially if their ecommerce website is an instance on a shared web hosting platform.

2 Taken from: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1_SAQ_A_rev1-1.pdf

The ecommerce integration methods that help a merchant's website fulfil the SAQ A-EP criteria include those described as: Silent Order Post, Direct Post, JavaScript created forms.

With these methods, the merchant's ecommerce website does not receive cardholder data but "*does affect the security of the payment transaction and/or the integrity of the page that accepts the consumer's cardholder data*" and does "*control[s] how consumers, or their cardholder data, are redirected to a PCI DSS validated third party payment processor*"[3] ; processing of the cardholder data is handled by a validated PCI DSS compliant service provider. This is illustrated by the diagram of the Direct Post method below:



In this example, the payment page originates from the merchant website and is configured to force submission of the cardholder data direct from the browser to the payment processor. The payment page does not include the code to instruct the browser to submit the card data back to the merchant website. For example, this may be done by excluding the `name` attribute in the form input fields representing the payment card data elements (card number, expiry date, security code, etc).

With the JavaScript created form method, the payment page configured by the merchant instructs the customer browser to request and execute some JavaScript from the payment solution provider. Unlike the Direct Post, if you were to inspect the source code of the merchant payment page you would not see form input fields representing the payment card data elements, like those shown in the sample above; however, inspection of the web page would reveal that third party JavaScript was being called to create the payment form elements appearing in the customer browser. The cardholder enters their payment card data into the JavaScript created form which is sent directly to the payment processor.

The process flows for the Direct Post and JavaScript created form methods are nicely illustrated in the Visa Processing E-Commerce Payments Guide and in the PCI SSC's Best Practice for Securing E-commerce information supplement.

3 Reference: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1_SAQ_A-EP_rev1-1.pdf

Client Side Encryption: An SAQ A-EP eligible ecommerce method?

A number of PSPs offer 'Client Side Encryption' (CSE). CSE is an ecommerce method whereby the consumer's payment card data is encrypted in the browser before being sent to the merchant's web server for onward submission to the PSP for processing. Merchants often like to use CSE as they retain complete control of their customer's ecommerce checkout experience but with no need to handle unencrypted payment card data.

The merchant website creates the payment form, including the PSP's JavaScript client encryption library using a `<script>` tag. When the consumer submits the payment form, the client encryption library, delivered from the PSP, intercepts the form submission and strongly encrypts the payment card fields. When the PSP receives the encrypted card data from the merchant, they decrypt it and process the transaction. Only the PSP has access to the decryption keys; the encrypted payment card data cannot be decrypted by the consumer, the merchant or any attacker.

CSE is regarded as SAQ A-EP eligible because the merchant does have an impact on the security of the payment transaction; the payment page originates from the merchant. Although the merchant does accept cardholder data on their website (per SAQ D), as that data cannot be decrypted by any entity except the PSP, this handling of encrypted payment card data is not deemed to negate SAQ A-EP eligibility.

The key difference between SAQ A eligible integration methods (discussed above) and SAQ A-EP eligible methods is:

- SAQ A: the payment page delivered to the customer browser originates in its entirety and directly from the validated PCI DSS compliant third party service provider. No element of the payment page originates from the merchant website.
- SAQ A-EP: form elements on the payment page may be created by HTML loaded from the merchant's website or by JavaScript loaded by the consumer's browser from the validated PCI DSS compliant third party service provider.

If any element of the payment page originates from anywhere other than the merchant website or a PCI DSS compliant service provider, then the implementation is not eligible for either SAQ A or SAQ A-EP. This is confirmed in PCI SSC FAQ 1293.

This expectation has raised concerns over merchants use of Google Tags on their payment pages. Google Tags are placed on a page to enable traffic analysis and marketing optimisation.

Use of Google Tags on a merchants' payment page – as opposed to the checkout page or other pages previous to the payment page - will negate eligibility for SAQ A or SAQ A-EP, as these tags would be page elements originating from a source that is not the merchant or a validated PCI DSS compliant third party service provider.

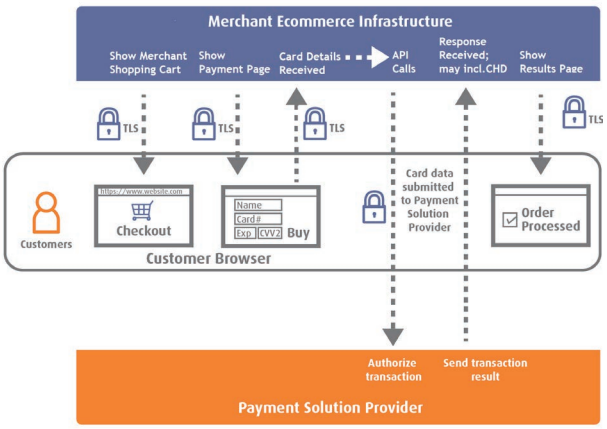
SAQ D

SAQ D applies to SAQ eligible ecommerce merchants where the merchant website is involved in both the acceptance and processing of the cardholder data.

SAQ D applies to SAQ eligible merchants that are unable to meet the eligibility criteria of the other SAQ types.

For ecommerce merchants, SAQ D may be applicable because:

- Customers enter their payment card details into a payment page presented by the merchant's website and that website receives the card data submitted by the customer; and/or,
- The merchant website stores cardholder data; and/or,
- The merchant website receives cardholder data back from the payment processor post-authorisation



The diagram above illustrates a typical direct integration website that requires assessment against SAQ D. It can clearly be seen that:

- The page requesting submission of and capturing payment card data originates from the merchant website (from the merchant domain)
- The card data submitted by the customer is received by the merchant website
- The merchant website controls the submission of the cardholder data to the PSP

Note: One legacy of PCI DSS v2.0 is the belief amongst many merchants and their ecommerce service providers that SAQ D will be applicable to ecommerce websites only if cardholder data is being stored. This mistaken belief has often led, for implementations like that shown in the diagram above, to the selection of SAQ C for assessment. This is demonstrably incorrect:

- SAQ C specifically states that it *"is not applicable to e-commerce channels"*
- SAQ D states that SAQ D is applicable to: *"E-commerce merchants who accept cardholder data on their website"*

Conclusion

Sysnet's QSAs are finding that the payment solution providers are developing payment integration methods that stretch or go right up to the bounds of the guidance and definitions provided in the SAQs and PCI SSC FAQs SAQ A and A-EP. This creativity can make determination of the appropriate SAQ incredibly difficult.

This guide has illustrated some of the common methods used, the distinguishing features of each and shown how they relate to the criteria and definitions of the ecommerce SAQs. In many cases however a detailed investigation of the code and method may be required to make a determination of the correct SAQ selection. A familiarity with your web browser's developer tools is most useful in undertaking any such investigation.

Further Reading

Ecommerce integration options and their PCI DSS compliance implications are explained in:

- Visa Europe e-commerce guide to security and PCI DSS requirements – diagrams and articulates PCI DSS scoping and assessment requirements applicable to different ecommerce integration types:
- PCI SSC FAQs:
  - Why is SAQ A-EP used for direct post while SAQ A is used for iFrame or URL redirect?
  - Why is there a different approach for direct post implementations than for iFrame and URL redirect?
  - If a merchant's ecommerce implementation meets the criteria that all elements of the payment page originates from a PCI DSS compliant service provider, is the merchant eligible to complete SAQ A or SAQ A-EP?
  - How is the payment page determined for SAQ A merchants using iframe?
  - Is a merchant website still in scope for PCI DSS if it meets all the criteria for SAQ A?
  - How do PCI DSS Requirements 2 and 8 apply to SAQ A merchants?

- PCI SSC Information Supplement: Best Practices for Securing E-commerce Guidelines
- MasterCard PCI Whitepaper
- Visa Data Security Alert (hosted payment pages)
- Web Browser Developer Tools:
  - Mozilla Firefox: https://developer.mozilla.org/en-US/docs/Tools/Page_Inspector
  - Microsoft Edge: https://developer.microsoft.com/en-us/microsoft-edge/platform/documentation/f12-devtools-guide/
    Google Chrome: https://developers.google.com/web/tools/chrome-devtools/

"Sysnet builds and supports mutually beneficial relationships between our clients and their customers globally through market-leading software, end-to-end services and best-in-class support."

Email: info@sysnetgs.com
Phone: +353 1 495 1300 | +1 404 991 3110
Web: sysnetgs.com

sysnet global solutions