# TSYS SECUR-ePAYMENT (TSEP):

## EXECUTIVE SUMMARY

AVIK MUKHERJEE | QSA, QSA (P2PE), CISSP, CHFI

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | coalfire.com

TSYS®

# EXECUTIVE SUMMARY

## OVERVIEW

TSYS, Inc. (TSYS) engaged Coalfire Systems, Inc. (Coalfire), a Payment Card Industry (PCI) Qualified Security Assessor Company (QSAC), to conduct an independent technical assessment of the TSYS Secur-ePayment (TSEP), an ecommerce payment application. Coalfire conducted technical testing, an architectural assessment, a compliance baselining relative to the PCI Data Security Standard (DSS), and peer review of the application.

Coalfire describes how the usage of TSEP aplication can reduce the risk of payment card data compromise within a merchant's ecommerce environment and reduce the scope of PCI Data Security Standard (DSS) validation when properly deployed. Possible scope reduction is based on proper implementation of TSEP and alignment to the PCI DSS 3.2 requirements. TSEP uses the TSYS PCI DSS compliant TransIT hosted environment for payment processing.

## AUDIENCE

This assessment report has two target audiences:

1. **Merchants:** This audience is looking for ecommerce payment processing solutions that can seamlessly integrate with their ecommerce platform and are in process of evaluating the TSEP solution for deployment in their payment card environment. Merchants will be able to clearly understand what benefits they can receive from using TSEP in their environment, including risk and scope reduction.
2. **Qualified Security Assessors** (**QSAs) and the Internal Audit Community**: This audience may be evaluating the TSEP application to determine the impact of usage of such application on PCI DSS compliance in general on behalf of their merchant.

## ABOUT TSYS SECUR-ePAYMENT

TSEP is a card-not-present application that helps merchants solve initial data capture and cardholder data (CHD) storage challenges by preventing CHD from entering their systems using client side encryption and subsequent tokenization of Primary Account Number (PAN) by TSYS within their PCI DSS validated service provider environment. This significantly reduces the threat of account data compromise and the infrastructure in scope for PCI DSS assessment.

# SUMMARY FINDINGS AND CONCLUSIONS

## FINDINGS

The following are highlights of Coalfire's technical evaluation of TSEP web application. NOTE: For the full context, the full technical paper should be reviewed**.** Please refer to TSYS website for the technical whitepepar on TSEP:

- Merchant web applications integrate with TSEP payment fields hosted by TSYS over HTTPS using URL redirect. Merchant web application achieves this trhough usage of  tags and <script> tag, script tag wold have the TSEP URL and will direct merchant web application to TSEP. The  tags gets replaced with TSEP hosted payment fields. When properly implemented, this can provide a secure method to handle CHD between a consumer and a payment processor, thereby allowing the merchant to keep their PCI DSS compliance effort to bare minimum.

- The TSEP application authenticates the merchant web application request using “Manifest” (an AES 256-bit encrypted string created by the merchant’s application) data and the merchant domain from which the request originates. The domain is registered during onboarding of the merchant. This provides an additional layer of protection by the TSEP web application to ensure it is serving legitimate requests and not requests from compromised/impersonated merchant web applications.
- Merchant web applications using TSEP hosted-payment fields do not receive plain-text PAN. This allows the merchant to reduce their PCI DSS scope to the minimum.
- The RSA 2048-bit public/private key strengths, used for encrypting the PAN while being consumed through users web browser, meets the PCI DSS standards for strong encryption and key management. This enables TSEP to derive the benefits of using encryption to reduce a significant portion of PCI DSS controls remaining for a merchant to manage on a consistent basis.
- Public Key Infrastructure (PKI) key management processes of the TSEP application relieves the merchant of the overhead of key management responsibilities.
- The TSEP application and associated manifest generation is provided by TransIT SDK including the transport channel encryption used between the merchant web application and TSEP. Thus, merchants do not have to invest their own resources to meet PCI DSS requirements related to secure coding practices and ensuring security of CHD in motion over untrusted networks. This is fulfilled by TSYS as their ecommerce solution provider.
- At the time of publication of this white paper, the TSEP backend payment processing and gateway environment was validated separately against PCI DSS v3.2 and found to be compliant with all PCI DSS controls (TSYS Acquiring Solutions Attestation of Compliance). TSEP is assessed against PCI DSS controls annually as part of TSYS Acquiring Solutions.
- TSEP returns a token in place of the PAN to the merchant web application, which in turn can be used by the merchant web application to communicate to TransIT MultiPASS$^{SM}$ server for further payment processing and backoffice activities such as refund, charge backs, or other financial reporting and analysis. As merchants are not handling PAN, those processes and infrastructure would not fall under merchant PCI DSS compliance scope.

## MERCHANT PCI DSS COMPLIANCE APPLICABILITY

Merchants using TSEP-hosted payment fields within their web application payment page can greatly lower their PCI DSS compliance effort through by reducing the threat exposure of their web application platform with respect to security of CHD. As with the TSEP application, TSYS is responsible for the following critical functions that ensure the security of the CHD:

- Security of the JavaScript and hosted payments fields used by TSEP. TSYS additionally provides TransIT SDK to be used by the merchant for generation of the initial manifest used in authenticating the merchant application request.
- Security of the RSA 2048-bit public/private key pair used by TSEP for encrypting and decrypting CHD. TSYS is responsible for the secure key management of those keys.
- The security of the implementation of the above points was validated as part of TSYS Acquiring Solutions PCI DSS compliance having AOC dated 04/11/2017, at the time of this publication.

Coalfire, after conducting a thorough evaluation of the TSEP application, concludes the following in terms of PCI DSS requirement applicability for a merchant:

- Level 1 merchants can qualify for PCI DSS scope reduction for their web application environment where CHD is not electronically stored, processed, or transmitted on systems when their web

application solely uses TSEP-hosted payment fields integration to handle all CHD responsibilities. Eligible merchant environments with TSEP can be validated against applicable controls to the SAQ A-EP for PCI DSS v3.2, which currently corresponds to much fewer PCI DSS control validation when compared to SAQ-D, which applies to merchants hosting and managing their in-house ecommerce payment processing application.

- Level 2, Level 3, and Level 4 merchants, defined by the payment brands that do not electronically store, process, and transmit CHD in their web application environment and implement TSEP-hosted payment fields, can be eligible for SAQ A-EP in alignment with the PCI DSS 3.2 standard. Merchants are required to consult their Acquirer(s) or payment brands about individual PCI DSS validation requirements and their eligibility for submitting an SAQ A-EP, which currently corresponds to much fewer PCI DSS control validation when compared to SAQ-D, which applies to merchants hosting and managing their in-house ecommerce payment processing application.

The conclusion is based on the PCI DSS SAQ eligibility, "Understanding the self-assessment questionnaires (SAQs) for PCI DSS version 3", found at the following site: (https://www.pcisecuritystandards.org/documents/Understanding_SAQs_PCI_DSS_v3.pdf).

The following summary chart provides a view of how the TSEP application may fulfill the PCI DSS v3.2 SAQ A-EP eligibility criteria, assuming the TSEP application has been properly implemented. Merchant environments can differ and it is important to work with the QSA to validate appropriate PCI DSS control reduction before making assumptions on scope reduction.

| PCI DSS SAQ A-EP ELIGIBILITY CRITERIA | TSEP APPLICATION CHARECTERISTIC |
|---|---|
| The merchant accepts only card-not-present (ecommerce or mail/telephone-order) transactions. | Provided the merchant is solely using TSEP-hosted payment field application for their ecommerce payment channels and the merchant does not have any other electronic payment channels. |
| All processing of cardholder data, with the exception of the payment page, is entirely outsourced to a PCI DSS validated third-party payment processor. | Merchant would be using TSYS as their third party PCI DSS validated payment processor. TSYS would handle processing of all cardholder data on the merchant's behalf including hosting and managing the payment fields.. |
| Merchant e-commerce website does not receive cardholder data but controls how consumers, or their cardholder data, are redirected to a PCI DSS validated third-party payment processor | Merchant using TSEP hosted payment fields manage how users are redirected to TSEP by including the TSEP URL in the merchants ecommerce application using HTML <script> tags. |
| If merchant website is hosted by a third-party provider, the provider is validated to all applicable PCI DSS requirements (e.g., including PCI DSS Appendix A if the provider is a shared hosting provider). | This would be dependent on how merchant hosts their web application. TSYS TSEP as a third party provider would not host the merchant web application and would only host the payment field to be used by merchant web application. If merchant chooses a third party service provider to host their web application, the merchant has to ensure that the service provider has all applicable PCI DSS validation completed. |
| 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) | All elemnets of the payment page (PAN, Expiry date and SAD), used by merchant, would originate from TSEP application hosted by TSYS, which is a PCI DSS validated service provider. |
| The merchant does not electronically store, process, or transmit any cardholder data on | The merchant web page provides only the landing page to the customers and all cardholder data processing is done on the client |

| | |
|---|---|
| merchant systems or premises, but relies entirely on a third party(s) to handle all these functions. | browser using the TSEP application and at backend by the TransIT host. |
| The merchant has confirmed that all third-party(s) handling storage, processing, and/or transmission of cardholder data are PCI DSS compliant. | TSYS handles processing of all cardholder data on the merchant's behalf and the TSYS TransIT environment is PCI DSS validated having a current AOC. |
| Any cardholder data the merchant retains is on paper (for example, printed reports or receipts), and these documents are not received electronically. | The merchant may store cardholder data on paper media while applying appropriate PCI DSS controls for security of the data. |

The Coalfire observations are in line with the recently released PCI SSC Information Supplement: PCI DSS E-commerce Guidelines
https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf

Section 2.2 of the information supplement document explains how using JavaScript based redirection in Shared-Management E-commerce environment provides greater risk reduction, which leads to merchant being eligible for SAQ A-EP for PCI DSS v3.2.

## ABOUT TSYS INC.

TSYS® (NYSE: TSS) is a leading global payments provider, offering seamless, secure and innovative solutions across the payments spectrum — from issuer processing and merchant acquiring to prepaid program management. We succeed because we put people, and their needs, at the heart of every decision. It's an approach we call 'People-Centered Payments®'.

Headquarters are located in Columbus, Ga., U.S.A., with approximately 11,500 team members and local offices spread across 13 countries. TSYS generated revenue of $4.2 billion in 2016, while processing more than 25.5 billion transactions. TSYS is a member of The Civic 50 and were named one of the 2017 World's Most Ethical Companies by Ethisphere magazine. TSYS is a member of the S&P 500 and routinely posts all important information on its website. For more, visit tsys.com.

## ABOUT THE AUTHOR

**Avik Mukherjee** | Senior Consultant

Avik is a Senior Consultant for the Coalfire Payment Processing P2PE group and assists clients in achieving compliance with the PCI Data Security Standard (PCI DSS) including Point-to-Point Encryption solution (P2PE). Avik has over eight years' experience in compliance, security technology design, and consultation. He earned his Master's degree in Business Administration and Bachelor's in Computer Engineering and holds Industry recognized certifications such as CISSP and CHFI.

Published July 2017.

## ABOUT COALFIRE

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. Coalfire.com



WP_TSYS Secur-ePayment Summary_072017