CFXWorks’ PCI DSS Position Paper

CFXWORKS, INC

2015

http://www.cfxworks.com

CFXWorks' PCI DSS Position Paper

Global Payments' OpenEdge / CFXWorks' PaymentCardXpress™ Relationship

CFXWorks' **PaymentCardXpress** (**PCX**) payment solution is implemented using Global Payments' PA DSS certified OpenEdge payment gateway. OpenEdge supports EMV enabled devices, Point to Point Encryption devices (P2PE), and hosted payment form (HPF) technologies. OpenEdge is designed to reduce fraud and protect card issuers, merchants and consumers from losses due to the use of counterfeit and stolen payment cards. OpenEdge's P2PE technology ensures that card holder data is protected from the point-of-entry throughout the payment process. HPF technologies eliminate the need for the merchant, and the merchant's payment solution, to ever process, capture, transport, store or process the primary account number (PAN), the expiration date, and the card code.

Card-Present:

For card-present transactions that are captured using EMV enabled point-of-sale devices, OpenEdge supports EMV Smart Cards and EMV enabled point-of-sale devices. EMV Smart Cards are embedded with a chip that interacts with a merchant's point-of-sale device, ensuring the card is valid and belongs to the user. This chip technology is said to be virtually impossible for a perpetrator to duplicate. Both EMV and P2PE technologies require the use of approved and certified peripherals.

Card-Not-Present:

For card-not-present transactions, the OpenEdge Hosted Payment Form (HPF) technology completely eliminates the Primary Card Number (PAN) from being captured, transported, stored, or processed by CFXWorks. This technology also eliminates the need for the merchant to capture, transported, store, or processed the PAN. For Card-Not-Present transactions deployed using OpenEdge's Hosted Payments Form (HPF) technology, certified peripherals are not required.

P2P Encryption (P2PE):

OpenEdge's proprietary encryption is designed to render cardholder data unreadable, encrypted at the point-of-entry. Merchants are unable to view card numbers after the swipe or hand-key.

Token Vault:

Cardholder data is replaced by digital "tokens" based on the OpenEdge technology. Sensitive data is stored in the secure OpenEdge vault rather than in the merchant environment. The **PCX** software stores the token and never has access to the PAN. A criminal attempting to steal cardholder data from a merchant's system would instead, find themselves with a useless invaluable token.

PaymentCardXpress is OUT-OF-SCOPE for PA-DSS 3.1

Because the Primary Account Number (PAN) is never captured, transported, stored, or processed by either PCX, or users of this solution, PCX is considered to be "Out-of Scope" relative to PCI DSS. This helps reduce cumbersome PCI validation requirements for both CFXWorks and our merchants. All merchants still have PCI validation responsibilities. The software provided by CFXWorks and Global Payments addresses only part of the PCI DSS responsibilities. Merchants still have to complete Merchant Level validation, but using an "Out of Scope" payment solution will make life much easier for them.

Global Payments PCI ASSURE Offering:

For merchants wanting added protection, Global Payments offers a program called EdgeShield, designed to help merchants simplify PCI compliance with online access to security self-assessment questionnaires, network scans, and custom security profiles generated from the business' processing activity. PCI ASSURE includes breach insurance to help merchants protect their businesses.

CFXWorks, Inc.

303 Arbor Green Lane

Alpharetta, GA 30004

678-455-0952

http://www.cfxworks.com

http://www.cfxworks-coldfusion.com

http://www.enterprise.com