A K-Rise Systems White Paper

K-Rise Systems

Enterprise. Easier.

EASYPay v4.8 – New Functionality, SaaS Enabled & More!

Removes PCI Scope from your LAN & Enables SAQ Form A

Companies realize credit card breaches & cyber-crime affects their potential liability with asking for their customers' credit card data. Both credit card automation & PCI security needs to be factored into your JDE credit card solution decision.

EXCLUSIVE: EASYPay v4.8 is the **first full SaaS cloud (Rackspace) credit card solution to the JDE community**. When considering where to locate (on premises vs. cloud) your company's credit card server… when factoring all the implications with cardholder data / PCI Scope (systems subject to a PCI audit), outsourcing is the better option. Customers also have the option of deploying EASYPay on premises.

EASYPay is completely re-architected to exclusively use payment gateway hosted payment forms so all cardholder data is removed from our customer's LAN. This approach enables our customers to complete SAQ Form A (not D) for compliance regulations (review PCI DSS section for more detail.)

EASYPay v4.8 JDE Credit Card Automation/Security Functionality:

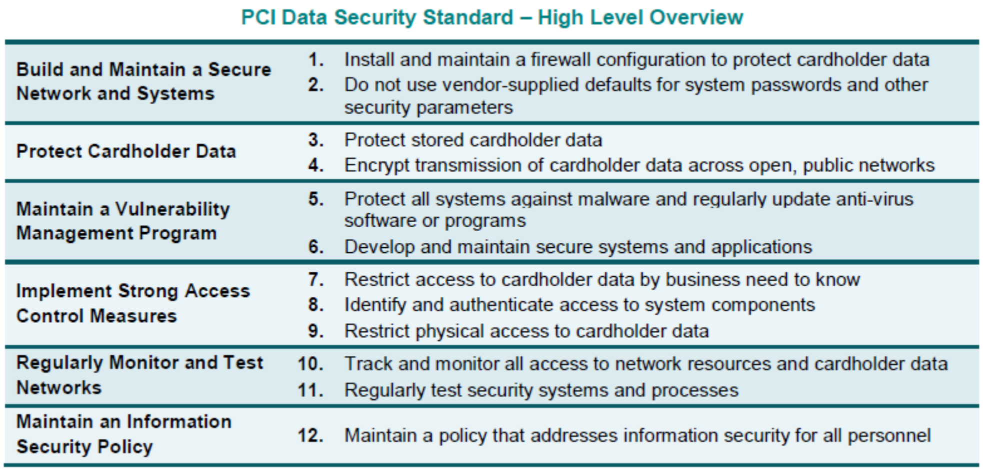
- **JDE Credit Card Sales Orders** for either P4210 or P42101
- **JDE Invoices "Collections" Payment**, Full or Partial / Single or Multiple Invoices
- **Tokenization** – Storage of Card Data at the Payment Gateway for Future Use - Allowing for Subsequent Orders and Follow-Up Transaction Usage – Can't be Reverse Engineered
- **Hosted Payment Forms** so Data Entry & Processing Occurs at the Payment Gateway
- **E-Commerce JDE Web Sales Orders** with EASYCommerce or any Storefront Solution like Magneto
- **Email Confirmation & Alerts**: Triggered Email, Sophisticated Workflow
- **Split-Payment Functionality** across Multiple Cards
- **Order-To-Cash**: Full Automation for: *Authorization*, *Settlement/Capture* and *Batch A/R Update*
- **Multiple Payment Gateways/Processors**: Authorize.Net, CyberSource, Moneris, BluePay, etc.

EASYPay v4.8 SaaS Deployment: Benefits:

- **Security** – The Rackspace data center is a PCI-DSS Compliant Infrastructure
- **Simple** – Because K-Rise Systems takes care of all the infrastructure set-up and security, it means that you can concentrate on running your business
- **Environments with Version Management** – EASYPay implementations involve three environments: Development, Test/QA and Production. These environments already exist with multi-tenant SaaS deployment.
- **Quick Implementation** – With no project infrastructure concerns, start to go-live can be accomplished in as little as 3-4 weeks.
- **Compliance** - Reduced PCI scope simplifies mandatory PCI DSS compliance requirements and reduces associated operating costs
- **Cost Savings** – Virtual or Physical Windows IIS & SQL servers are expensive especially when factoring Microsoft maintenance. All that is eliminated with SaaS

A review of PCI DSS Consortium relevant information & SAQ Detail:

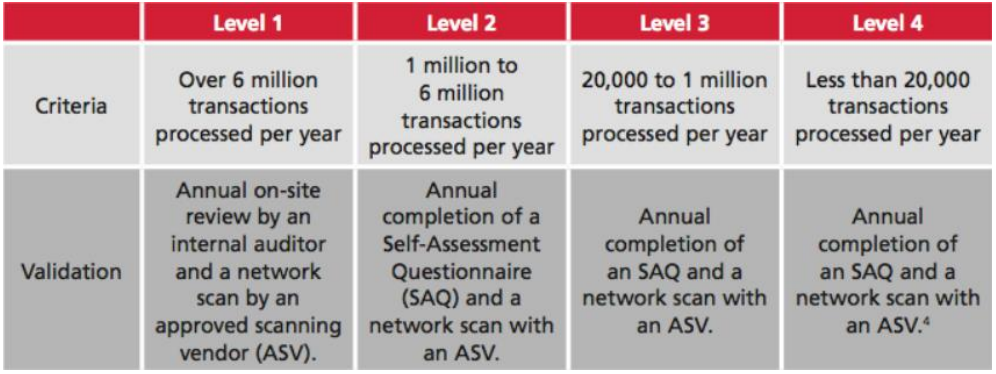
- CHD = Cardholder Data
- CDE = Cardholder Data Environment
- Hosted Payment Page – Refers to a payment data entry page, that users are directed to, that is completely hosted by the Payment Gateway. The hosted payment page can be branded like the rest of your site – only the URL is different.
- The PCI DSS 12 Requirements Documents can be viewed by clicking here. In general they are:



PCI Data Security Standard – High Level Overview

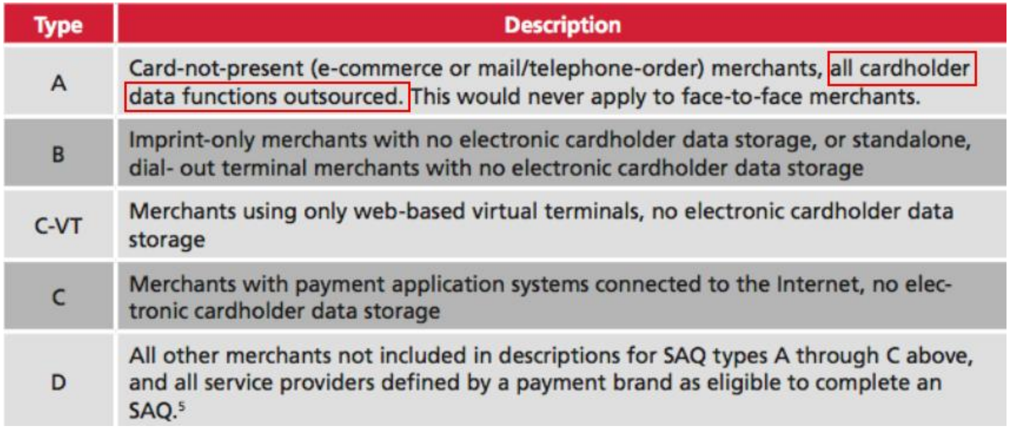
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

- PCI-DSS Merchant Levels And Validation Types



	Level 1	Level 2	Level 3	Level 4
Criteria	Over 6 million transactions processed per year	1 million to 6 million transactions processed per year	20,000 to 1 million transactions processed per year	Less than 20,000 transactions processed per year
Validation	Annual on-site review by an internal auditor and a network scan by an approved scanning vendor (ASV).	Annual completion of a Self-Assessment Questionnaire (SAQ) and a network scan with an ASV.	Annual completion of an SAQ and a network scan with an ASV.	Annual completion of an SAQ and a network scan with an ASV.[4]

- Validation Level Determines which SAQ (Self-Assessment Questionnaire) Type you need to complete



Type	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial- out terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ.[5]

◆ Defining: "Cardholder Data Functions Outsourced" - PCI rules talk at length about:

- Data being **Processed**
- Data in **Transmit** Stage
- Data in Storage

The official PCI Instructions and Guidelines document explaining **your** responsibilities for completing the annual SAQ document can be reviewed by clicking here. Because of card breaches, cybercrime, etc. Banks are becoming increasingly diligent with enforcing this PCI compliant mandate to their customers. Most JDE companies fall under the "card not present" PCI categories which means they would either need to complete the very simple (13 questions) PCI DSS SAQ (Self-Assessment Questionnaire) Form A or the extremely complex (288 questions) SAQ Form D. Form D is especially difficult for mid-size businesses who generally work without a Compliance business operation.

From the PCI SAQ instruction guide: "**SAQ A – Card-not-present Merchants, All Cardholder Data Functions Outsourced**: *"SAQ A has been developed to address requirements applicable to merchants who retain only paper reports or receipts with cardholder data, do not store cardholder data in electronic format and **do not process or transmit any cardholder data** on their systems or premises*."

EASYPay v4.8 **exclusively** utilizes the payment gateway "hosted payment form" for credit card entry. The users: (1) CSR for E1 P4210 sales orders and (2) Web Buyers for e-commerce orders are both entering the credit card data in an iFrame based payment gateway hosted payment form (that's company branded so they don't realize they are entering the data at the gateway). Thus the card **processing**, **transmit** and **tokenization storage** occurs entirely at the payment gateway. This fact allows EASYPay companies to complete the simple SAQ Form A. In fact because EASYPay v4.8 no longer manages cardholder data, our solution per PCI QSA's (Qualified Security Assessor) is no longer a "Payment Application" subject to PCI PA-DSS Validation, - - it's middleware.

Other JDE credit card solution providers require CSRs to enter customer card data on a JDE system form. Other approaches involve entering the card data on a form associated with the on premises credit card server. The vendors focus on the tokenized storage of the card data at the gateway. They do not focus on the underlying processing tables (even if used for a millisecond to process & transmit for gateway tokenization/storage) related to the card entry form. Those tables reside on your LAN and put JDE and any other connected systems in: "PCI Scope" with those systems subject to a PCI audit. Those tables could also be exposing your customers' data, "in the clear" a potential PCI compliance concern.