Sterling Selling and Fulfillment Foundation

Sterling Sensitive Data Capture Server, Release 1.1: PA-DSS Implementation Guide

Release 9.1.0.24

Sterling Selling and Fulfillment Foundation

Sterling Sensitive Data Capture Server, Release 1.1: PA-DSS Implementation Guide

Release 9.1.0.24

Note

Before using this information and the product it supports, read the information in “Notices” on page 31.

Copyright

This edition applies to the 9.1 Version of IBM Sterling Selling and Fulfillment Foundation and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Roadmap: Using the PA-DSS, Secure Deployment, and SSDCS Documentation Guides

The IBM® Sterling Selling and Fulfillment Foundation provides a strategy for secure credit card capture and protection, in accordance with the Payment Application Data Security Standard (PA-DSS) and the Payment Card Industry Data Security Standard (PCI DSS).

If your deployment captures credit cards, you can implement the IBM Sterling Sensitive Data Capture Server (SSDCS) to capture credit card numbers on behalf of the IBM applications. Doing so ensures that credit card numbers are kept outside of IBM Sterling Selling and Fulfillment Suite applications, with the added benefit that these applications are kept outside of PCI DSS auditing scope.

The following guides in the Sterling Selling and Fulfillment Foundation documentation set discuss how to implement these security strategies:

- *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide* (this guide) - Describes the steps to follow for your SSDCS installation to remain in compliance with the PA-DSS. It also describes order capture and payment processing data flows, as well as showing a typical network implementation of the SSDCS. This guide explains how to keep the Sterling Selling and Fulfillment Suite applications outside of the PCI DSS auditing scope.
- *Sterling Selling and Fulfillment Foundation: Secure Deployment Guide* - Explains how to deploy the Sterling Selling and Fulfillment Foundation securely. It covers security recommendations for applications, networks, operating systems, databases, application servers, and message queues.
- *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide* - Details how to install, configure, and deploy SSDCS as a proxy service that IBM applications call to tokenize Primary Account Numbers (PANs) for credit cards and gift value cards.

Implementation Sequence

To implement these strategies, IBM suggests that you follow this sequence of steps:

1. Review all three guides in this order:
   a. *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide*
   b. *Sterling Selling and Fulfillment Foundation: Secure Deployment Guide*
   c. *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide*
2. Implement the steps suggested in the *PA-DSS Implementation Guide* to remain in compliance with PA-DSS and keep your IBM applications outside of the PCI DSS auditing scope.
3. Implement the security strategies outlined in the *Sterling Selling and Fulfillment Foundation: Secure Deployment Guide*.
4. Install Sterling Selling and Fulfillment Foundation and associated applications (refer to the *Sterling Selling and Fulfillment Foundation: Installation Guide* and respective application installation guides).

5. Follow the steps in the *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide* to configure your SSDCS implementation.

Chapter 2. About the PA-DSS Implementation Guide

The *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide* describes the steps that you must follow for your Sterling Sensitive Data Capture Server (SSDCS) installation to remain in compliance with the Payment Application - Data Security Standard (PA-DSS). It also describes how to keep the IBM applications outside of the PCI Data Security Standard (PCI DSS) auditing scope.

The information in this document is based on the PCI Security Standards Council (PCI SSC) PA-DSS program (Version 2.0, dated October, 2010). IBM recommends that you deploy the SSDCS application in a manner that adheres to the PCI DSS and the PCI PA-DSS, Version 2.0.

Subsequent to this, best practices and hardening methods such as those referenced by the Center for Internet Security (CIS), including their various "Benchmarks," should be followed to enhance system logging, reduce the chance of intrusion, and increase the ability to detect intrusion. Other general recommendations to secure networking environments should be followed, as well. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, disabling of infrequently used or frequently vulnerable networking protocols, and the implementation of certificate-based protocols for access to servers by users and vendors.

Note: If you do not follow the steps outlined here, your Sensitive Data Capture Server installations will not be PA-DSS compliant and the IBM applications could be considered to be within PCI DSS auditing scope.

Sterling Sensitive Data Capture Server PA-DSS Implementation Guide Revision Information

Revision Information	
Author	Bernie Wong, Application Security Advisor
Approving Authority	Steven Aulds, Director of Development and SaaS Operations, IBM Commerce
Revision Date	March 31, 2011
Next Review Date	March 31, 2012, or whenever the underlying application changes, or whenever the PA-DSS requirements change
Exclusions	Applies to all Engineering employees who develop or maintain the SSDCS

Sterling Sensitive Data Capture Server PA-DSS Implementation Guide Update History

Name	Title	Date	Summary of Changes
Bernie Wong	Performance Engineering Director	Dec 14, 2009	Initial version
		October 15, 2010	Version update

Name	Title	Date	Summary of Changes
		March 31, 2011	Updated for SSDCS Release 1.1

The *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide* will be reviewed on a yearly basis, whenever the underlying application changes, or whenever the PA-DSS requirements change. IBM will distribute this guide to new customers in the product documentation DVD. In addition, IBM will provide updates.

Chapter 3. Overview of the PA-DSS Implementation Guide

The Sterling Sensitive Data Capture Server is a proxy service that applications call to tokenize Primary Account Numbers (PANs) for credit cards and store gift value cards. The term "tokenization", as used in this document, refers to the process of replacing a sensitive PAN with a unique string token. With tokenization, the PAN or store gift value card numbers are stored in a credit card vault, and the tokens are stored in the applications of IBM.

Currently, the following applications of IBM have been architected to use the SSDCS:

- IBM Sterling Distributed Order Management, Release 9.1
- IBM Sterling Call Center, Release 9.1, and IBM Sterling Store, Release 9.1
- IBM Sterling Field Sales, Release 9.1

The Sterling Sensitive Data Capture Server application, Release 1.1, has been certified with Payment Application Data Security Standard (PA-DSS) Version 2.0 by Coalfire Systems Inc., a Payment Card Industry (PCI) SSC-approved Payment Application Qualified Security Assessor (PAQSA).

This document also explains the PCI initiative and the PA-DSS guidelines. The document provides specific installation, configuration, and ongoing management best practices for using Payment Application as a PA-DSS-validated application operating in a PCI-Compliant environment.

PCI Security Standards Council Reference Documents

The following documents provide additional details surrounding the PCI SSC and related security programs, such as PA-DSS and PCI DSS:

- Payment Applications Data Security Standard (PA-DSS) and the Payment Card Industry Data Security Standard (PCI DSS)
  Both standards are available from:
  https://www.pcisecuritystandards.org/security_standards/
- Open Web Application Security Project (OWASP)

Sterling Sensitive Data Capture Server Application Summary

Application Feature	Description
Name	Sterling Sensitive Data Capture Server (SSDCS)
Application Version Number	1.1
Components of the Application, such as POS and Back Office	The Sterling Selling and Fulfillment Foundation applications use the Sterling Sensitive Data Capture Server to convert credit card and other sensitive information to tokens for security. The applications are Sterling Field Sales, Sterling Call Center, Sterling Store, and Sterling Distributed Order Management.

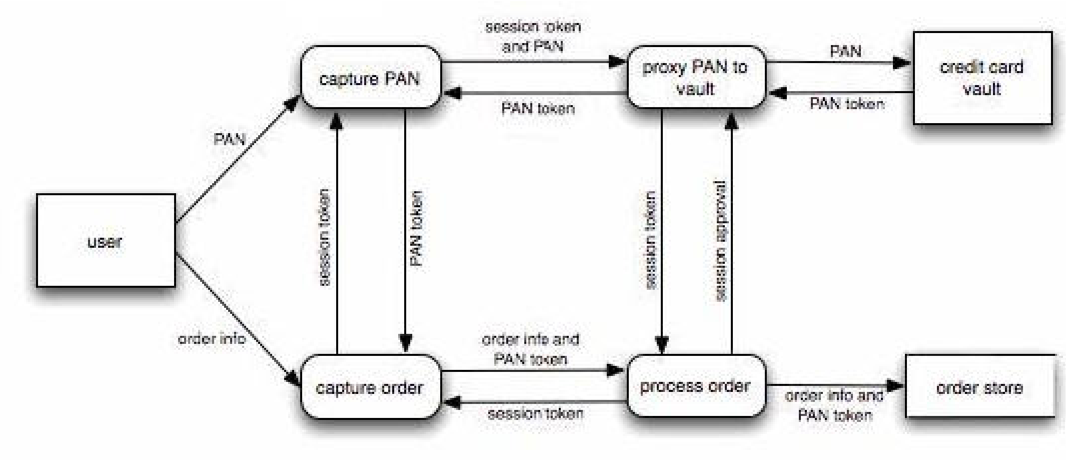
Application Feature	Description
Credit Card Server(s)	The Sterling Sensitive Data Capture Server does not use credit card servers.
Other Required Third-Party Software	The Sterling Sensitive Data Capture Server is designed to serve as a Web-based proxy service to credit card vaults. The SSDCS requires the following software components: • a J2EE application server • Java • Apache log4j • OWASP Enterprise Security API Refer to the *Sterling Selling and Fulfillment Foundation: System Requirements Guide* for the supported version numbers.
Setup	Components of the Application, such as POS and Back Office. The SSDCS runs as a service in a J2EE application server. The SSDCS installation and configuration steps are documented in the *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide*.
Operating Systems	The Sterling Sensitive Data Capture Server is currently supported on the following operating systems: • Red Hat Linux • IBM AIX® • HP HP-UX • Sun Solaris • SUSE Linux • Microsoft Windows Server 2008 Refer to the *Sterling Selling and Fulfillment Foundation: System Requirements Guide* for the current supported version numbers.
Code Base, DB Engine	The Sterling Sensitive Data Capture Server does not use a database engine.
Application Description	The Sterling Sensitive Data Capture Server is a service that the Sterling Field Sales, Sterling Call Center, Sterling Store, and Sterling Distributed Order Management applications call to tokenize and store credit card and gift card numbers in a credit card vault. As part of the proxy service, the SSDCS authenticates and validates the request.

Application Feature	Description
Application Environment	The Sterling Sensitive Data Capture Server should run in the DMZ if it is a service to Internet users. This server should run in the Internal or Trusted network if it is a service to internal users. These deployment options are described in the topic, "Typical Network Implementation" and in the *Sterling Selling and Fulfillment Foundation: Secure Deployment Guide*. The SSDCS is a Web application running in a J2EE application server. The SSDCS does not use or rely on a database server.
Application Target Clientele	The SSDCS is a PAN tokenization service to the following IBM applications: • The Distributed Order Management system is used by organizations that want to manage orders captured in a single or multi-sales channel. • The Sterling Call Center and Sterling Store applications are used to implement call center and store functionalities such as order capture, order status, and order modification. • The Sterling Field Sales application provides complex order capture and order quoting functionality.
Description of Versioning Methodology	IBM releases major versions of the Sterling Selling and Fulfillment Foundation product on a regular basis. These releases use a naming convention with a number format V.R., where V refers to Version and R refers to Release numbers. Between these releases, the Sterling Selling and Fulfillment Foundation applications regularly release fix packs to address customer issues and bugs identified in the field. These use the naming convention V.R.0.x, with the x denoting the fix pack release.

Chapter 4. Data Flow Diagram Depicting the Order Capture Data Flow

This section describes the flow of cardholder data or Payment Application Number (PAN) for an order capture and a payment authorization transaction.

The following Data Flow diagram shows the order capture function.



In this illustration, the flow of PAN and order information takes two distinct paths.

First Path:

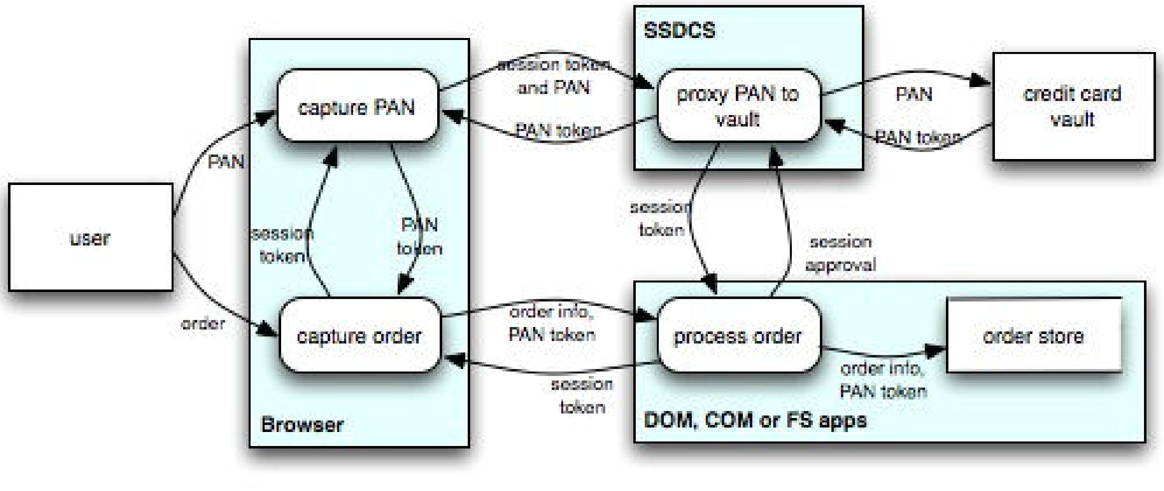
1. Sensitive PAN information from the *user* is sent to the capture PAN.
2. This information is then sent to the proxy PAN to vault process.
3. The information goes to the credit card vault for storage.

Second Path:

1. The captured order information flows from the user to the capture order process.
2. During the capture order process, the PAN token from the first path and the order information are sent to the process order process.
3. The order information and PAN token are stored in the order store.

The key point here is that second path does not touch or process sensitive PAN information.

The following illustration shows how the processes in the previous Order Capture Data Flow illustration are partitioned into the Sterling Distributed Order Management (DOM), Sterling Call Center and Sterling Store (COM), and Sterling Field Sales applications (FS apps).



In terms of software partitioning, the PAN is captured in the browser separately from the order information, as follows:

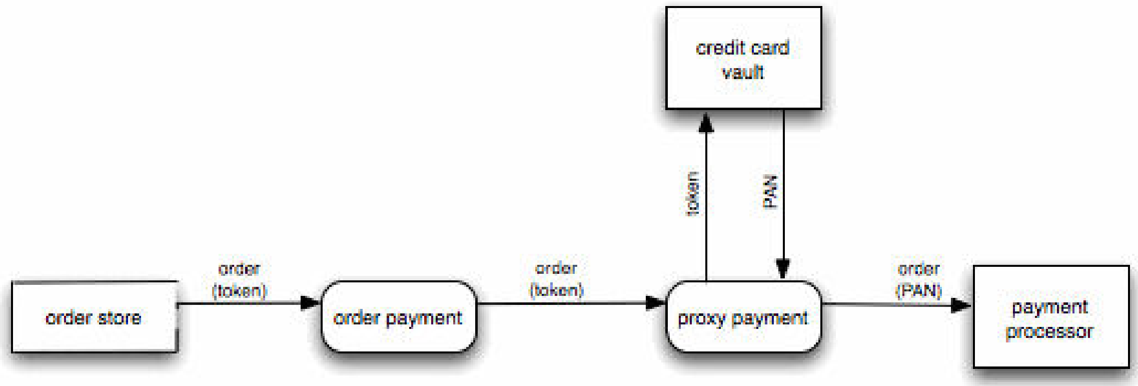
1. From the browser, PAN information is sent to the SSDCS as a tokenization request.
2. This tokenization request, in turn, sends the PAN to the credit card vault.
3. The credit card vault tokenizes and stores the PAN and returns a token.

The second path from the browser to the actual DOM, COM, or SF applications contains only the order information and PAN token, not the actual, cleartext (unencrypted) PAN. As a result, the order store contains only tokens.

From a PCI PA-DSS and PCI DSS perspective, the flows in the previous two illustrations are important, showing that architecturally, the DOM, COM, and FS applications do not touch PAN. This means that these applications may be kept outside of the PCI DSS auditing scope.

Payment Processing Transaction Example

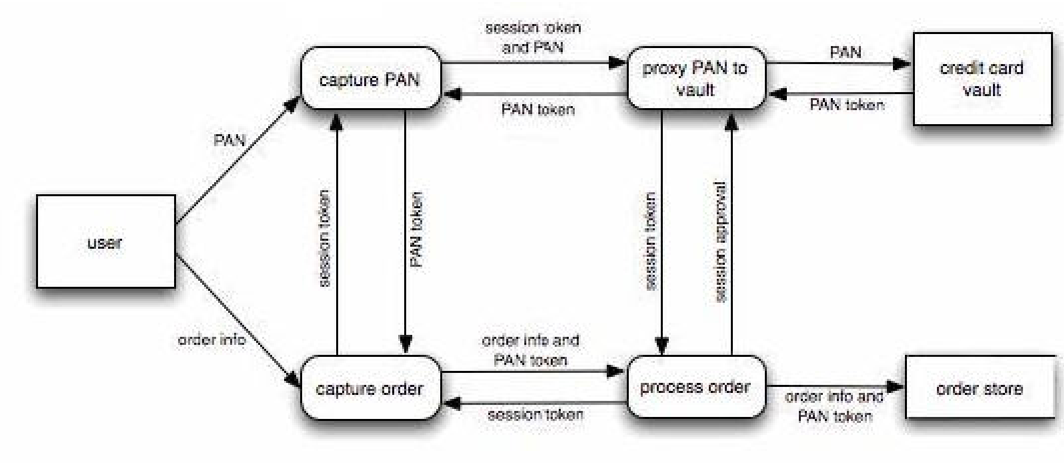
The following diagram illustrates a Payment Processing Transaction.



In this Payment Processing Transaction illustration, the order payment process prepares an order that requires payment authorization for transmission to a payment processor as follows:

1. Because the order store has only tokens, the order payment process sends the payment request with the token to the proxy payment process.
2. The proxy payment process detokenizes the token back to the cleartext (unencrypted) PAN, and replaces the token in the payment request.
3. The proxy payment process then forwards the payment request to a payment processor.

In the following illustration, the data flow diagram shown in the previous illustration is partitioned into software components.



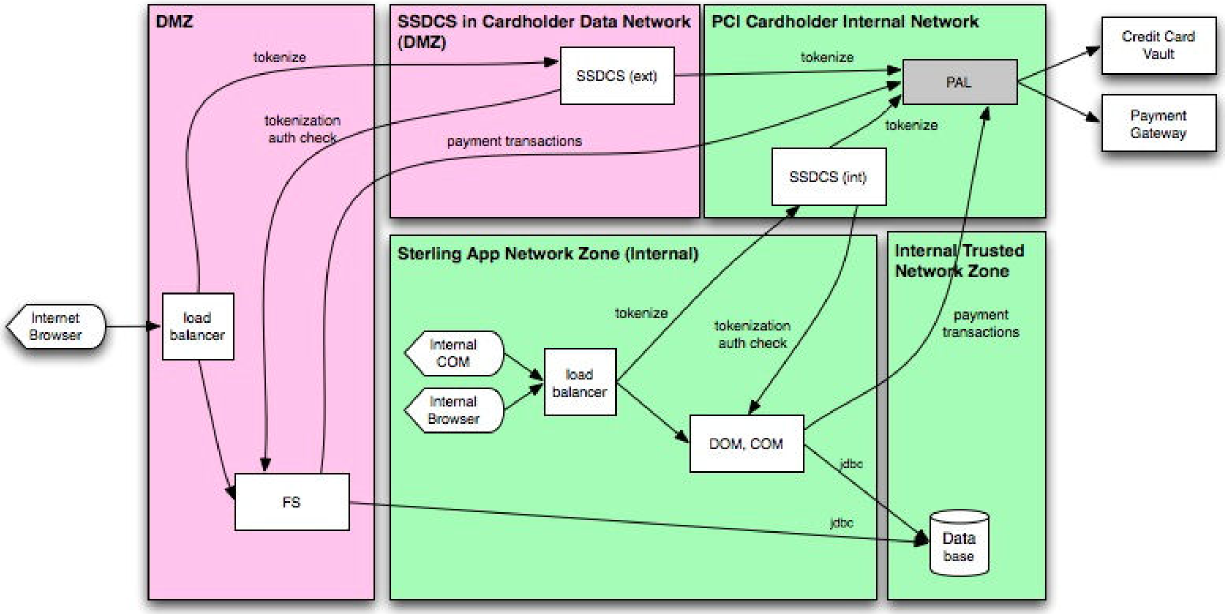
In this illustration, the task of detokenization is delegated to a component called the Payment Abstraction Layer (PAL). This is a customer-provided component. This partitioning approach serves two critical purposes:

- The places where tokens can be converted to PAN are limited and controlled.
- This approach ensures that the IBM applications do not have access to PAN, and therefore, cannot process PAN. As a result, the IBM applications can be kept outside of the PCI DSS auditing scope.

Chapter 5. Typical Network Implementation

This topic describes one possible network implementation of the Sterling Sensitive Data Capture Server along with the Sterling Field Sales, Sterling Call Center, Sterling Store, and Sterling Distributed Order Management applications. The *Sterling Selling and Fulfillment Foundation: Secure Deployment Guide* presents alternative network implementation strategies. You should consult this guide if your implementation has a different mix of application components, or if you want to place your application components in more restricted network security zones as a result of your security risk assessment.

The following diagram illustrates a typical network implementation.



In the implementation shown in this illustration, the IBM applications perform the following roles:

- Sterling Field Sales (FS) enables users to create quotes for complex orders.
- Sterling Distributed Order Management (DOM) provides order fulfillment functionality, such as performing payment authorization, picking fulfillment channels, and so forth.
- Sterling Call Center and Sterling Store (COM) enable internal call center and store representatives to create and manage orders. Orders (and credit card information) can be entered through one of the following three channels:
  - Internet-based users, such as sales representatives, generate complex sales quotes and then proceed to create the orders through the Sterling Field Sales (FS) applications.
  - Internal Sterling Distributed Order Management (DOM) users, such as customer service representatives, enter orders through the DOM console.

- Internal DOM users, such as customer service representatives, enter orders through the RCP-based Sterling Call Center and Sterling Store (COM) application.

As the previous illustration shows, any of these applications that touches credit card data or PANs should reside inside the SSDCS DMZ PCI Cardholder Network. Cardholder data is kept away from the database and the Payment Abstraction Layer (PAL), which reside in the Internal Trusted Network Zone and the Internal PCI Cardholder Network, respectively. Because the PAL performs all of the tokenization and detokenization requests for payment processing, it can be monitored and securely protected, while the application sees only the order and the token, keeping the application in a PCI-compliant environment.

For browser-based applications, refer to the *Sterling Selling and Fulfillment Foundation: Secure Deployment Guide* and to the *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide* for more information about how to integrate Sterling Sensitive Data Capture Server with IBM applications.

Chapter 6. Difference Between PCI Compliance and PA-DSS Validation

The responsibility of IBM as a software vendor is to be validated by the Payment Card Industry (PCI) Payment Applications Data Security Standard (PA-DSS).

IBM has performed an assessment and certification compliance review with an independent assessment firm to ensure that its platform conforms to industry best practices when handling, managing, and storing payment-related information.

PCI PA-DSS is the standard against which Payment Applications have been tested, assessed, and validated.

PCI DSS Compliance is later obtained by the merchant, and is an assessment of your actual server (or hosting) environment.

Obtaining PCI DSS Compliance is the responsibility of the merchant and your hosting provider, working together, using PCI-compliant server architecture with proper hardware and software configurations and access control procedures.

The PCI PA-DSS Validation is intended to ensure that the Payment Application will help you achieve and maintain PCI DSS Compliance with respect to how the Payment Application handles user accounts, passwords, encryption, and other payment data-related information.

The Payment Card Industry has developed security standards for handling cardholder information in a published standard called the "PCI Data Security Standard." The security requirements defined in the DSS apply to all members, merchants, and service providers who store, process, or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment, which is defined as any network device, host, or application that is included in or connected to a network segment where cardholder data is stored, processed, or transmitted.

PCI DSS and PCI PA-DSS in Relationship to Applications of IBM

The Sterling Sensitive Data Capture Server (SSDCS), the service component used by applications to tokenize PAN, has been PCI PA-DSS validated. You need to follow the instructions provided in this guide to ensure the SSDCS is implemented in such a manner that it remains PCI PA-DSS compliant.

The Sterling Distributed Order Management application has been architected to use the SSDCS so that it never captures, stores, processes, or transmits PAN. If you maintain this separation, you should be able to keep this application outside the scope of PCI auditing.

The Twelve Requirements of the PCI DSS

The following list provides twelve PCI DSS requirements.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data.

2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

3. Protect stored data.

4. Encrypt transmission of cardholder data and sensitive information across public networks.

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software.

6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

7. Restrict access to data on a business need-to-know basis.

8. Assign a unique ID to each person with computer access.

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.

Chapter 7. Considerations for the Implementation of Payment Applications in a PCI-Compliant Environment

The security standards described in this section must be considered for proper implementation in a PCI-Compliant environment.

Remove Historical Credit Card Data (PA-DSS 1.1.4)

PA-DSS 1.1.4 states that historical data such as magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the software must be securely deleted. Removal of these data is absolutely necessary for PCI compliance.

The Sensitive Data Capture Server proxies tokenization requests to your credit card vault and does not store sensitive authentication data. Therefore, there is no historical credit card information to remove from the SSDCS application, as required by PA-DSS Version 2.0.

Sensitive Authentication Data Requires Special Handling (PA-DSS 1.1.5)

PA-DSS 1.1.5 states that the following guidelines must be followed when dealing with sensitive authentication data (swipe data, validation values or codes, PIN or PIN block data):

- Collect sensitive authentication data only when required to solve a specific problem.
- Store such data only in specific, known locations with limited access.
- Collect only the limited amount of data required to solve a specific problem.
- Encrypt sensitive authentication data while stored.
- Securely delete such data immediately after use.

This requirement does not apply to the SSDCS because it neither collects nor stores card authentication data.

Purging of Cardholder Data (PA-DSS 2.1)

PA-DSS 2.1 states that cardholder data must be purged after it exceeds the customer-defined retention period from all locations where payment application stores cardholder data. The Sterling Sensitive Data Capture Server does not store cardholder data; therefore, there is no data to be purged, as required by PA-DSS Version 2.0.

For any cardholder data you store outside of the SSDCS, you should develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes. Purge (render irretrievable) any stored cardholder data as retention thresholds are met.

Customers who currently store PAN in the associated Sterling Distributed Order Management application will be have to replace PAN in their database with tokens when they incorporate the use of the Sterling Sensitive Data Capture Server. PCI compliance requires that these data be removed securely.

For the Sterling Distributed Order Management application, it is recommended that you use the following process:

1. Identify database tables that store PAN. Traditionally, these tables are YFS_PAYMENT and YFS_CUSTOMER_PAYMENT_METHOD.
2. Write an upgrade program to iterate through each payment method. For each of the payment methods with a PAN:
   a. Decrypt the PAN.
   b. Call the credit card vault to tokenize the PAN.
   c. Replace the PAN with the PAN token.

Be aware that as you replace your PAN data with tokens during the upgrade process, your PAN data will be found in many places in your database, such as your database's transaction logs, archive logs, undo tablespace (for Oracle), audit records, and backup tapes. As a result, there is a window of exposure during which your system may continue to contain sensitive PAN data, even after you convert all the PANs to tokens. Your window of exposure ranges from minutes to years, for the following reasons:

- PAN data in transaction logs (DB2® or SQL Server) and redo logs (Oracle) will persist until the transaction logs are reused. This could range from minutes to hours, depending on the number and size of the transaction logs and on your database update transaction volume.
- PAN data in Oracle's undo tablespace will persist until the undo records are reused. The estimated time to reuse the undo space cannot be determined.
- PAN data in transaction archive logs will persist until the archive logs are no longer needed and are reused, which could typically range from weeks to potentially months.
- PAN data in audit logs will persist until the audit records are purged or deleted. This could range from months to years depending on your audit retention policies.

Here are some suggested methods to securely purge cardholder data:

- Use eraser or secure delete with a NIST approved algorithm and purge all old logs/files/and or databases.
- Encrypt existing backups or create new backups and securely delete old iterations.
- Develop a manual procedure to over write PAN stored in databases three times, then drop or delete the data. For example:
  1. Enter 1111111111111111111s.
  2. Enter 0000000000000000000s.
  3. Enter 1010101010101010101s.
  4. Delete / Drop.
  5. Replace the data in field with Tokenized PAN.

Furthermore, we recommend based on your risk assessment and threat modeling, you perform the following to prevent the operating system from inadvertently capturing cardholder data:

- For Windows platform:
  – The System Backup/Restore operation can inadvertently write out cardholder data that was in memory at the time of system backup. To avoid this, the System Restore option should be disabled.

  - Clear the Windows paging file (Pagefile.sys) during the shutdown process, so that no unsecured data is contained in the paging file when the shutdown process is complete.

Refer to your Windows operational documentation for specific directions on how to perform these activities on your systems.

- For both Windows and Unix, the cardholder data in memory can be written out to page files or swap when memory is constrained. The amount of time that the data is in the page file/swap will be short, typically until the data in the Java Virtual Machine is garbage collected (rendered irretrievable).
- Refer to the *Selling and Fulfillment Foundation: Secure Deployment Guide* for further guidance on securing operating systems.

Key Management Roles and Responsibilities (PA-DSS 2.5 and PA-DSS 2.6)

PA-DSS 2.5 and PA-DSS 2.6 state that the payment application must implement key management processes and protect cryptographic keys used for encryption of cardholder data against disclosure and misuse. The Sterling Sensitive Data Capture Server does not store cardholder data, nor does it provide any configurability that would allow a merchant to store cardholder data. The SSDCS is a proxy interface that allows the Sterling Distributed Order Management application to off load Primary Account Numbers to your credit vault server in exchange for a surrogate token.

Similarly, the Sterling Distributed Order Management application does not store encrypted PAN. As a result, the SSDCS and IBM applications do not require key management roles and responsibilities, as they are related to the storage of encrypted credit card numbers.

Removal of Cryptographic Material (PA-DSS 2.7)

PA-DSS 2.7 states that cryptographic material must be removed. Such removal is absolutely necessary for PCI compliance.

Previous versions of Sterling Sensitive Data Capture Server never used encryption. As a result, there is no cryptographic data to be securely removed as required by PA-DSS Version 2.0.

You must remove all cryptographic material that the Sterling Distributed Order Management application used to encrypt PAN. If you are upgrading from an earlier version of these applications, it is your responsibility to identify and then remove the cryptographic material.

Set Up Access Controls (PA-DSS 3.1 and PA-DSS 3.2)

PA-DSS 3.1 requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process without the use of generic group accounts that are utilized by more than one user or processes.

You must assign strong passwords to any default accounts (even if they won't be used), and then disable or do not use the accounts. Do not use administrative accounts for application logins. For example, do not use the SQL System Administrator account for application access to the database.

The Sterling Sensitive Data Capture Server is a simple tokenization proxy that does not have defined users or roles. The SSDCS does not have any application users or administrators. As a result, there are no administrator users to manage in the SSDCS. You will, however, have to create operating system users to install and configure the SSDCS. You will also have to create an application server user to configure, manage, and run the application server in which the SSDCS operates.

The Sterling Sensitive Data Capture Server PA-DSS audit, meets or exceeds the requirements as outlined below.

For both the completion of the initial installation and for all subsequent changes (for example, any changes that result in user accounts reverting to default settings, any changes to existing account settings, or changes that generate new accounts or recreate existing accounts), you will need operating system and application server users. When you create or manage these users you have to adhere to the following 10 requirements as per PCI DSS 8.1, 8.2, and 8.5.8-15:

1. Must assign unique IDs for user accounts. (8.1).
2. Must provide at least one of the following three methods to authenticate users (8.2):
   a. Something you know, such as a password or passphrase
   b. Something you have, such as a token device or smart card
   c. Something you are, such as a biometric
3. Must NOT require or use any group, shared, or generic accounts or passwords.(8.5.8).
4. Require passwords to be changed at least every 90 days (8.5.9).
5. Require passwords must to be at least 7 characters (8.5.10).
6. Require passwords to include both numeric and alphabetic characters (8.5.11).
7. Require keeps password history and requires that a new password is different than any of the last four passwords used. (8.5.12).
8. Require limits repeated access attempts by locking out the user account after not more than six logon attempts. (8.5.13).
9. Lockout duration is set to a minimum of 30 minutes or until an administrator enables the user ID. (8.5.14).
10. Require the user to re-authenticate to re-activate the session if the application session has been idle for more than 15 minutes.

These same account and password criteria from the above 10 requirements must also be applied to any applications or databases included in payment processing to be PCI compliant.

Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.

PA-DSS 3.2 states that you must control access, via unique username and PCI DSS-compliant complex passwords, to any PCs or servers with payment applications and to databases storing cardholder data.

Train and Monitor Administrative Personnel

It is your responsibility to institute proper personnel management techniques for allowing administrative user access to credit cards, site data, and so forth. You can control whether each individual administrative user can see all the credit card PANs (or only the last 4).

In most systems, a security breach is because of unethical personnel. So pay special attention the people you trust your administrative site with and to those whom you allow to view full decrypted and unmasked payment information.

Audit Trails and Centralized Logging (PA-DSS 4.1 and PA-DSS 4.4)

PA-DSS 4.1 states that Payment Applications must set PCI DSS-compliant log settings, per PCI DSS Requirement 10. In addition, logs must be enabled, and disabling the logs will result in noncompliance with PCI DSS.

The Sterling Sensitive Data Capture Server has PA-DSS-compliant logging enabled by default. This logging is not configurable and cannot be disabled.

Note: Disabling or subverting the logging function of the Sterling Sensitive Data Capture Server in any way will result in noncompliance with PCI DSS.

The Sterling Sensitive Data Capture Server's logging is configured per PCI DSS 10.2 and 10.3 as follows:

- Implement automated assessment trails for all system components to reconstruct the following events:
  - 10.2.1 All individual user access to cardholder data
  - 10.2.2 All actions taken by any individual with root or administrative privileges
  - 10.2.3 Access to all assessment trails
  - 10.2.4 Invalid logical access attempts
  - 10.2 5 Use of identification and authentication mechanisms
  - 10.2.6 Initialization of assessment logs
  - 10.2.7 Creation and deletion of system-level objects
- Record at least the following assessment trail entries for all system components for each event from 10.2.x:
  - 10.3.1 User identification
  - 10.3.2 Type of event
  - 10.3.3 Date and time
  - 10.3.4 Success or failure indication
  - 10.3.5 Origination of event
  - 10.3.6 Identity or name of affected data, system component, or resource.

Out of the box, the Sterling Sensitive Data Capture Server writes logs to a directory that is dictated by the log4j properties. Customers must develop the capability to automatically copy these logs to their centralized log server. For more information about how to set the log4j properties, refer to the *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide* and the *Sterling Selling and Fulfillment Foundation: Properties Guide*.

Note: With respect to PCI DSS 10.2.7, except for the creation of the application logs for logging and auditing purposes, the SSDCS does not create other system-level objects such as files or directories.

The files created during the installation or upgrade processes can be tracked by running the installation steps in verbose mode. For more information about the installation steps, see the *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide*.

In order to comply with PCI DSS 10.2.7, implement an external monitoring program, typically called host-based intrusion detection systems (HIDS) to detect changes to the file system. An example of such a tool is the Open Source Tripwire. The discussion of the use and configuration, or selection of the external monitoring tools is beyond the scope of this document.

Use of Necessary and Secure Services, Protocols, Daemons, Components, and Dependent Software (PA-DSS 5.4)

PA-DSS 5.4 states that Payment Applications must only use or require the use of necessary and secure services, protocols, daemons, components, and dependent software and hardware, including those provided by third parties, for any functionality required by the payment application (such as NetBIOS, file sharing, Telenet, FTP, or others) and that these should be secured via SSH, S-FTP, SSL, IPSec, or other technology.

The SSDCS is a simple J2EE-based proxy to the customer's credit card vault or payment abstraction layer. The only service it requires is access to the HTTPS port.

Customers may want to enable the remote non-console access to administer the application or system. IBM recommends that customers use only secure protocols, such as SSH and SCP.

PCI-Compliant Wireless Settings (PA-DSS 6.1 and PA-DSS 6.2)

PA-DSS 6.1 and PA-DSS 6.2 state that if wireless is used within the payment environment, you should install a firewall, according to PCI DSS Requirement 1.3.8.

The Sterling Sensitive Data Capture Server does not support wireless technologies. However, should the merchant implement wireless access within the cardholder data environment, the following guidelines for secure wireless settings must be followed according to PCI Data Security Standards 1.2.3, 2.1.1, and 4.1.1, which are described in this section.

PCI Data Security Standard 1.2.3

Perimeter firewalls must be installed between wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

PCI Data Security Standard 2.1.1

- All wireless networks must implement strong encryption; for example, Advanced Encryption Standard (AES).

- Encryption keys must be changed from default at installation, and changed every time that a person with knowledge of the keys leaves the company or changes positions.
- Default Simple Network Management Protocol (SNMP) community strings on wireless devices must be changed.
- Default passwords and pass phrases on access points must be changed.
- Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks, such as WPA and WPA2.
- Other security-related wireless vendor defaults apply, if appropriate.

PCI Data Security Standard 4.1.1

- Industry best practices must be used to implement strong encryption for the following over the wireless network in the cardholder data environment:
  - Transmission of cardholder data
  - Transmission of authentication data
- Payment applications using wireless technology must facilitate the following for use of Wired Equivalent Privacy (WEP):
  - For new wireless implementations, implementing WEP has been prohibited as of March 31, 2009.
  - For current wireless implementations, using WEP is prohibited after June 30, 2010.

Never Store Cardholder Data on Internet-Accessible Systems (PA-DSS 9.1)

PA-DSS 9.1 states that payment applications must not store cardholder data on Internet-accessible systems. For example, a Web server and database server must not be on the same server.

The Sterling Sensitive Data Capture Server does not store cardholder data. The information in tokenization requests is not stored in the Sterling Sensitive Data Capture Server. The card's Primary Account Number is sent to your credit card vault for storage.

PCI-Compliant Remote Access Using Two-Factor Authentication (PA-DSS 10.2)

PA-DSS 10.2 requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism. The means two of the following three authentication methods must be used:

1. Something you know, such as a password or passphrase.
2. Something you have, such as a token device or smart card.
3. Something you are, such as a biometric.

PCI-Compliant Delivery of Updates (PA-DSS 10.3.1)

PA-DSS 10.3.1 states that payment applications that receive remote payment application updates through secure modems must conform to PCI DSS Requirement 12.3. In addition, computers must comply with PCI DSS Requirement 1 or 1.3.9 if they are connected through a VPN or other high-speed connections, in order to receive remote payment application updates through a firewall or a personal firewall.

As a development company, IBM keeps abreast of the relevant security concerns and vulnerabilities in our area of development and expertise. Once we identify a relevant vulnerability, we work to develop and test a fix pack that helps protect the Sterling Sensitive Data Capture Server against a specific, new vulnerability. We attempt to publish a fix pack within 30 days of a critical vulnerability being identified. We then contact vendors and dealers to encourage them to install the fix pack. Typically, merchants are expected to respond quickly to and install the available fix packs within 30 days.

We do not deliver software or updates or both through remote access to customer networks. Instead, software and updates are available through our secure customer portal, the Customer Center. Access to the portal is only granted to users with the appropriate authentication credentials.

IBM's Software Fulfillment will generate an MD5 and SHA-1 cryptographic hash value for each fix pack so that customers can verify fix pack integrity prior to installation.

PCI-Compliant Secure Remote Access (PA-DSS 10.3.2)

PA-DSS 10.3.2 requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token, certificate or biometric).

The SSDCS is designed to run in your data center either in a DMZ or a trusted network. However, the Sterling Sensitive Data Capture Server does not require or rely on secure remote access. If you choose to remotely manage the SSDCS, operating system or application server, then administrators in your corporate network must use secure protocols, such as Secure Shell (SSH), X11 Tunneling through SSH, and Secure File Transfer Protocol (SFTP) in order to connect to and administer the Sterling Sensitive Data Capture Server.

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

If users and hosts within the payment application environment need to use third-party remote access software, such as Virtual Networking Computing (VNC), Remote Desktop Protocol (RDP), or Symantec pcAnywhere, to access other hosts within the payment processing environment, special care must be taken. The Sterling Sensitive Data Capture Server does not require specialized remote access software. You should consider disabling these services for security hardening.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For environment need to use third-party remote access software, such as Virtual Networking Computing (VNC), Remote Desktop Protocol (RDP) this means using the high encryption setting on the server, and for Symantec pcAnywhere it means using symmetric or public key options for encryption. Additionally, the PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, you are advised to take the following precautions:

- Change default settings (such as user names and passwords) on remote access software (e.g. VNC)
- Allow connections only from specific IP and/or MAC addresses
- Use strong authentication and complex passwords for logins according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS 8.1, 8.3, and 8.5.8-8.5.15
- Enable encrypted data transmission according to PA-DSS 12.1 and PCI DSS 4.1
- Enable account lockouts after a certain number of failed login attempts according to PA-DSS 3.1.8 and PCI DSS 8.5.13
- Require that remote access take place over a VPN via a firewall as opposed to allowing connections directly from the internet
- Enable logging for auditing purposes
- Restrict access to customer passwords to authorized reseller/integrator personnel
- Establish customer passwords according to PA-DSS 3.1.1 – 3.1.10 and PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5

Data Transport Encryption (PA-DSS 11.1)

PA-DSS 11.1 states that payment applications must implement and use SSL for secure cardholder data transmission over public networks, in accordance with PCI DSS Requirement 4.1.

The PCI DSS requires the use of strong cryptography and encryption techniques with at least a 128-bit encryption strength at the transport layer with a Secure Sockets Layer (SSL) or Internet Protocol Security (IPSEC) layer; or at the data layer with algorithms such as RSA or Triple Data Encryption Standard (DES) to safeguard cardholder data during transmission over public networks (this includes the Internet and Internet-accessible DMZ network segments).

PCI DSS requirement 4.1: Use strong cryptography and security protocols such as SSL/Transport Layer Security (TLS) and IPsec to safeguard sensitive cardholder data during transmission over open, public networks.

Refer to the Order Capture Data Flow diagram in the topic “Data Flow Diagram Depicting the Order Capture Data Flow” for an understanding of the encrypted data flow associated with the Sterling Sensitive Data Capture Server.

The Sterling Sensitive Data Capture Server will process only tokenization requests that are secured with SSL/TLS. Requests that are not secured by SSL/TLS will be rejected and logged.

PCI-Compliant Use of End User Messaging Technologies (PA-DSS 11.2)

PA-DSS 11.2 states that payment applications must implement and use an encryption solution if PANs can be sent with end-user messaging technologies.

The Sensitive Data Capture Server does not, out of the box, provide the means to send PAN through end-user messaging technology, such as e-mail, instant messaging, and chat.

Nonconsole Administration (PA-DSS 12.1)

PA-DSS 12.1 states that Payment Applications must implement and use Secure Shell (SSH), Virtual Private Network (VPN), or SSL/TLS for encryption of any nonconsole administrative access to payment application or servers in a cardholder data environment.

There is no console access to the Sterling Sensitive Data Capture Server.

Nonconsole access to the computer server that the Sterling Sensitive Data Capture Server runs on should only be made through secure protocols such as SSH or secure tunneling protocols such as a VPN.

Nonconsole access to the application servers that the Sterling Sensitive Data Capture Server runs should only be made through the X Window protocol that is tunneled through SSH. By default, X Window events are sent in the clear.

The Sterling Sensitive Data Capture Server does not use insecure services such as NetBIOS, file sharing, Telnet, or unencrypted FTP to manage the application (as per PCI DSS Requirement 2.3).

Disseminate PA-DSS Implementation Guide (PCI PA-DSS 13.1)

PA-DSS 13.1 states that the payment application vendor must develop, maintain, and disseminate a *PA-DSS Implementation Guide*(s) for customers, resellers, and integrators.

The *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide* will be reviewed on a yearly basis, whenever the underlying application changes, or whenever the PA-DSS requirements change. IBM will distribute this guide to new customers in the product documentation DVD. In addition, IBM will provide updates.

Network Segmentation

The PCI DSS requires that firewall services be used with Network Access Translation (NAT) or Port Address Translation (PAT) to separate network segments into logical security domains based on the environmental requirements for Internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming Internet traffic to the trusted application environment can be allowed. Additionally, outbound Internet access from the trusted segment must be limited to required and justified ports and services.

Refer to the Order Capture Data Flow diagram in the topic "Data Flow Diagram Depicting the Order Capture Data Flow" for an understanding of the flow of encrypted data associated with the Sterling Sensitive Data Capture Server.

In the illustration in the topic "Typical Network Implementation", PAN information flows from the Internet user under SSL/TLS to the SSDCS in the cardholder data network, and then to the customer's credit card vault for tokenization. PAN information from Internal users flows to an internal SSDCS, which is in an internal cardholder data network for tokenization.

Tokens are used only in the IBM applications in the noncardholder data network.

Maintain An Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan that every merchant or service provider should adopt in developing and implementing a security policy and program:

- Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between the existing practices in your organization and those outlined by the PCI requirements.
- After the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.
- Create an action plan for ongoing compliance and assessment.
- Implement, monitor, and maintain the plan. Compliance is not a one-time event. Regardless of the merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.
- Call in outside experts, as required.

Chapter 8. Application System Configuration

Refer to the *Sterling Selling and Fulfillment Foundation: System Requirements Guide* for operating systems, dependent application patch levels, and configurations that are supported and tested for continued PCI DSS compliance.

Payment Application Initial Setup and Configuration

Refer to the *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide* for detailed instructions about how to install the SSDCS.

During the SSDCS installation, logging is enabled by default. You can modify the logging levels through the standard log4j properties. PA-DSS-compliant logging is discussed in Audit Trails and Centralized Logging (PA-DSS 4.1 and PA-DSS 4.4). Log4j information is documented in the *Sterling Selling and Fulfillment Foundation: Sterling Sensitive Data Capture Server, Release 1.1: Configuration Guide* and in the *Sterling Selling and Fulfillment Foundation: Properties Guide*.

The SSDCS is not built with an administrative interface. You can administer the SSDCS through the application server's administration console and through property files.

As a proxy, the SSDCS does not encrypt data. All PAN encryption, and as a result, all key management responsibilities, are delegated to the customer's credit card vault.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium and the Ultrium Logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Connect Control Center®, Connect:Direct®, Connect:Enterprise®, Gentran®, Gentran®:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, and Sterling Integrator® are trademarks or registered trademarks of Sterling Commerce™, Inc., an IBM Company.

Other company, product, and service names may be trademarks or service marks of others.

Index

Printed in USA