Sterling Sensitive Data Capture Server, Release 1.0

PA-DSS Implementation Guide

Selling and Fulfillment Foundation, Release 9.0

Last updated in HF15

January 2011

Sterling Commerce
An IBM Company

Notice and Disclaimer:

In this document, the terms “you,” “your,” or “yours” refer to the end user or the customer. The terms “we,” “our,” or “ours” refer to Sterling Commerce (America), Inc. (“Sterling Commerce,” “Sterling Commerce, Inc.,” or “Sterling”).

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to, PA-DSS and DSS.

The customer may undertake activities that may affect compliance. For this reason, Sterling Commerce, Inc. is required to be specific to only the standard software provided by Sterling.

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. STERLING COMMERCE MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER STERLING NOR ANY OF ITS REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION HEREIN.

STERLING COMMERCE DOES NOT AND CANNOT WARRANT OR REPRESENT THAT IMPLEMENTATION OF THE RECOMMENDATIONS, GUIDELINES, AND/OR DIRECTIONS HEREIN WILL RESULT IN A SECURE SYSTEM. THE INFORMATION HEREIN IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY, AND ARE ONLY SUGGESTIONS: NOTHING HEREIN SHOULD BE CONSTRUED AS PART OF ANY USER OR CUSTOMER GUIDE OR OTHER DOCUMENTATION AGAINST WHICH ANY CONTRACTUAL WARRANTY IS MADE, OR CAN BE CONSTRUED.

THE APPLICABLE STERLING COMMERCE ENTITY RESERVES THE RIGHT TO REVISE THIS PUBLICATION FROM TIME TO TIME AND TO MAKE CHANGES IN THE CONTENT HEREOF WITHOUT THE OBLIGATION TO NOTIFY ANY PERSON OR ENTITY OF SUCH REVISIONS OR CHANGES.

You are responsible for identifying the security options most appropriate to the risks identified in your environment.

This document assumes that you are familiar with security deployment concepts, including knowledge of how to deploy these applications securely. Specifically, you must ensure that the recommendations can be used in your corporate operational environment.

Sterling Commerce strongly recommends that you work with your internal or external security teams from the initial planning stages to production deployment. Most importantly, ensure that engineers knowledgeable in security are involved in designing the system, which includes the Sterling Commerce applications.

Contents

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

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 Sterling Sensitive Data Capture Server (SSDCS) to capture credit card numbers on behalf of the Sterling applications. Doing so ensures that credit card numbers are kept outside of Sterling applications, with the added benefit that these applications are kept outside of PCI DSS auditing scope.

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

- *PA-DSS Implementation Guide* (this guide) - Describes the steps that you should 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 applications outside of the PCI DSS auditing scope.
- *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 Sensitive Data Capture Server: Configuration Guide* - Details how to install, configure, and deploy SSDCS as a proxy service that Sterling Commerce applications call to tokenize Primary Account Numbers (PANs) for credit cards and gift value cards.

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

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

About the *PA-DSS Implementation Guide*

The *PA-DSS Implementation 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 Sterling Commerce 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 1.2, dated October, 2008). Sterling Commerce recommends that you deploy the SSDCS application in a manner that adheres to the PCI DSS and the PCI PA-DSS (version 1.2).

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 Sterling applications could be considered to be within PCI DSS auditing scope.

Sterling Sensitive Data Capture Server, Release 1.0: PA-DSS Implementation Guide Revision Information

Revision Information	
Author	Bernie Wong, Performance Engineering Director
Approving Authority	Steven Aulds, Senior Vice President, Engineering
Revision Date	March 31, 2010
Next Review Date	March 31, 2011, 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
Standard Number	ESP201

Sterling Sensitive Data Capture Server, Release 1.0: PA-DSS Implementation Guide Update History

Name	Title	Date	Summary of Changes
Bernie Wong	Performance Engineering Director	Dec 14, 2009	Initial version

The *PA-DSS Implementation Guide* ("IG") will be reviewed on a yearly basis, whenever the underlying application changes, or whenever the PA-DSS requirements change. Sterling Commerce will distribute this guide to new customers in the product documentation DVD. In addition, Sterling Commerce will provide updates through the Online Documentation Library at the Sterling Commerce Customer Center at the following URL:

https://cn.sterlingcommerce.com/login.jsp

Overview of the *PA-DSS Implementation Guide*

The Sterling Sensitive Data Capture Server is a proxy service that Sterling Commerce 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 Sterling Commerce applications.

Currently, the following Sterling Commerce applications have been architected to use the SSDCS:

- Sterling Web™, Release 9.0
- Sterling Distributed Order Management™, Release 9.0
- Sterling Call Center™, Release 9.0, and Sterling Store™, Release 9.0
- Sterling Field Sales™, Release 9.0

The Sterling Sensitive Data Capture Server application, Version 1.0, has been certified with Payment Application Data Security Standard (PA-DSS) Version 1.2 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)
  http://www.owasp.org

Sterling Sensitive Data Capture Server Application Summary

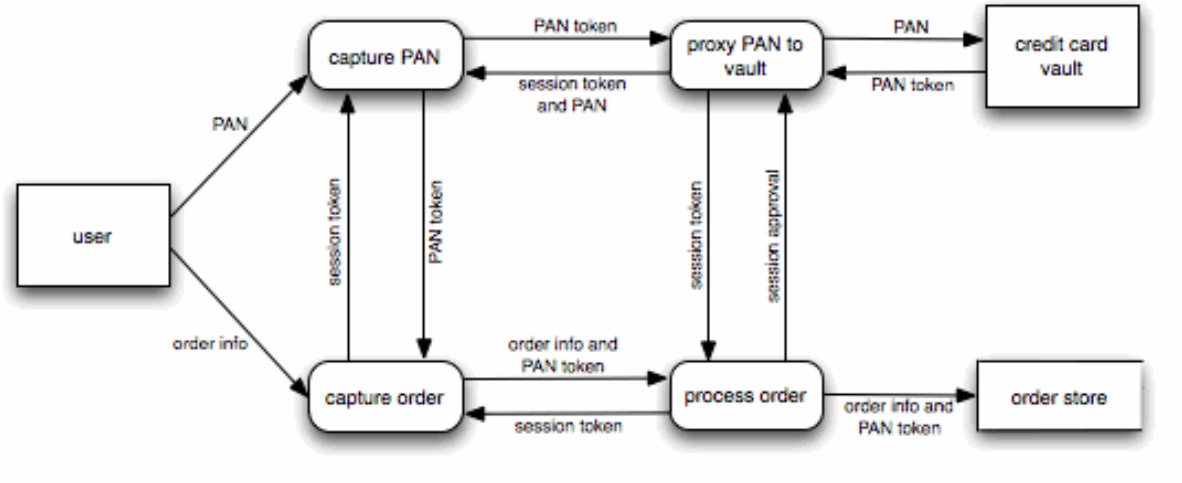
Application Feature	Description
Name	Sterling Sensitive Data Capture Server (SSDCS)
Application Version Number	1.0
Components of the Application, such as POS and Back Office	The Sterling Selling and Fulfillment Foundation applications use the Sterling Sensitive Data Capture Server to convert credit card and other sensitive information to tokens for security. The Sterling Selling and Fulfillment Foundation applications are Sterling Web, Sterling Field Sales, Sterling Call Center, Sterling Store, and Sterling Distributed Order Management.
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 Refer to the *Selling and Fulfillment Foundation: Installation 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 Sensitive Data Capture Server: 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™ Refer to the *Selling and Fulfillment Foundation: Installation 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 Web, 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 *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 Sterling Commerce applications: ◆ The Sterling Web application is used by B2C and B2B organizations that want to implement Internet shopping with product or item catalogs, shopping carts, and order capture functionality. ◆ 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	Sterling Commerce releases major versions of the 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 Selling and Fulfillment Foundation applications regularly release Service Packs and Hot Fixes to address customer issues and bugs identified in the field. These use the naming convention V.R SPx, with x denoting the Service Pack release, or V.R HFx, with the x denoting the Hot Fix release.

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:

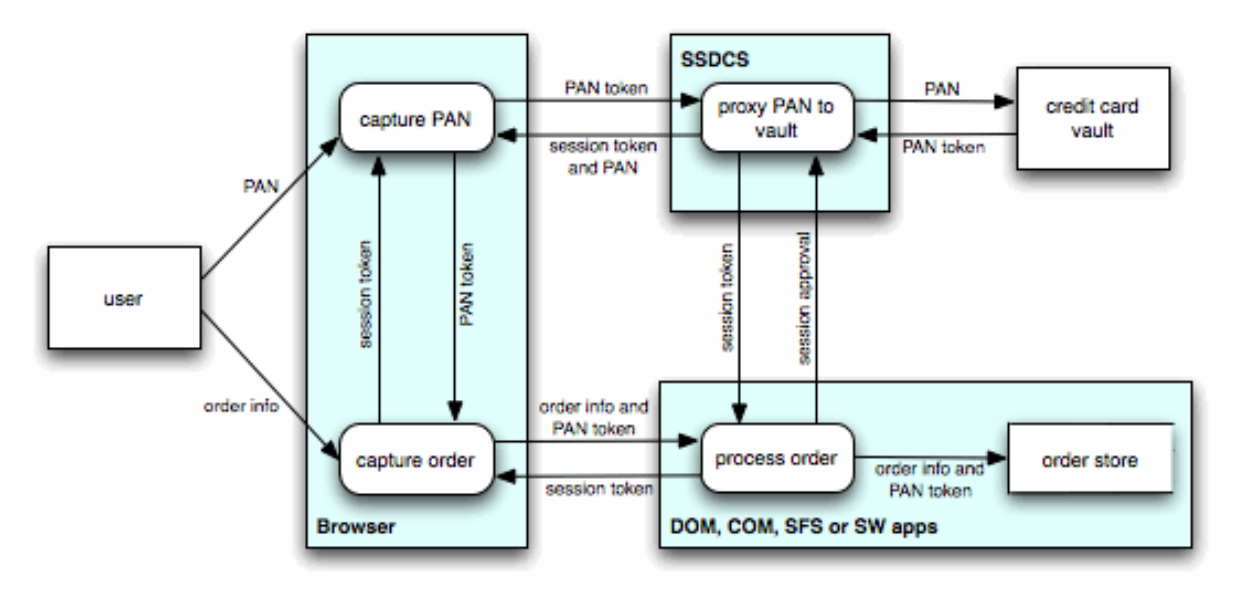
1. Sensitive PAN information from the *user* is sent to the capture PAN.
2. This information is then sent to the proxy PAN to vault process.
3. The information goes to the credit card vault for storage.

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 Field Sales (FS), or Sterling Web (SW).



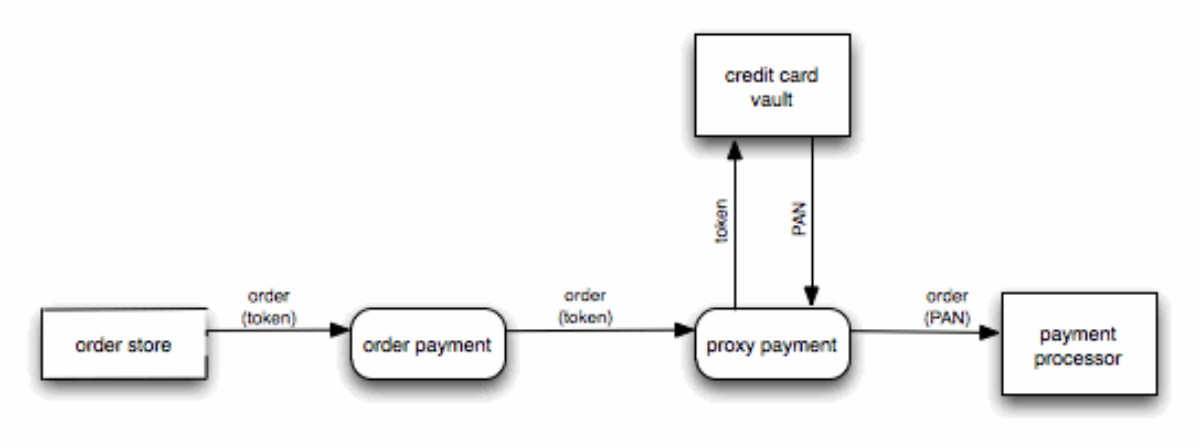
In terms of software partitioning, the PAN is captured in the browser separately from the order information, as follows:

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, FS, or SW 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, FS, and SW applications do not touch PAN. This means that these applications may be kept outside of the PCI DSS auditing scope.

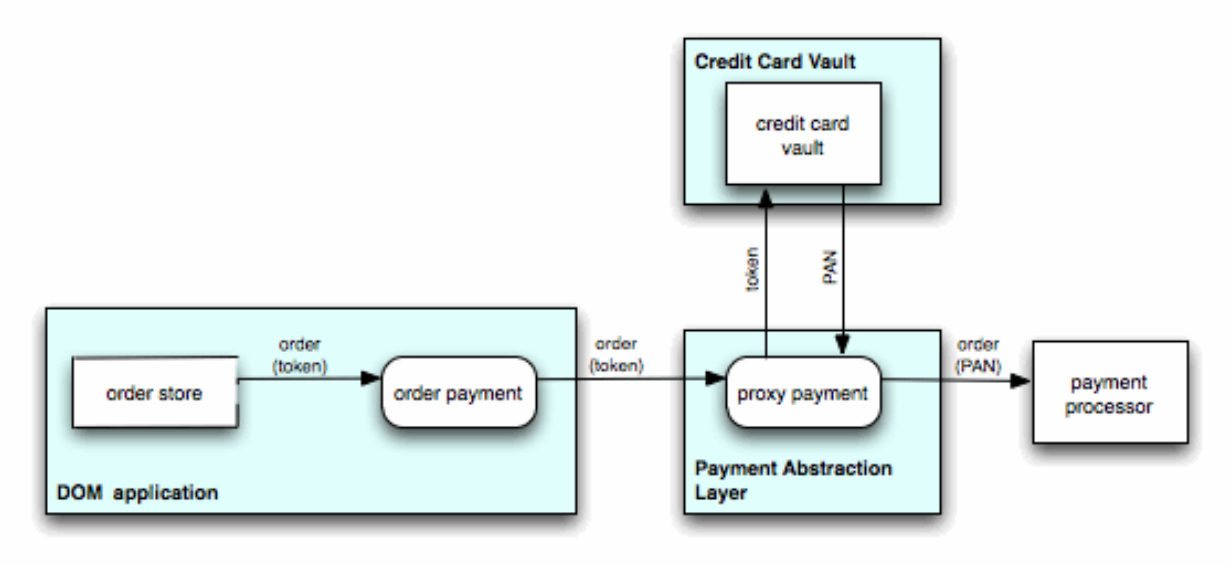
The following diagram illustrates a Payment Processing Transaction.



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.



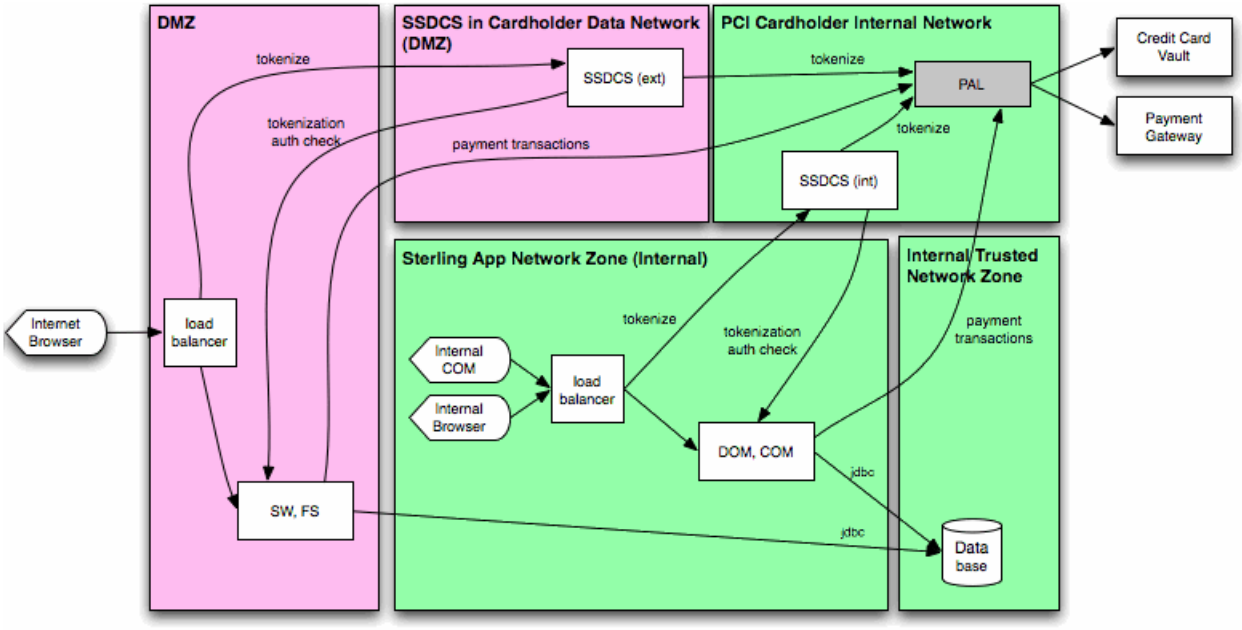
In this illustration, the task of detokenization is delegated to a component called the Payment Abstraction Layer (PAL). This is a customer-provided component. This partitioning approach serves two critical purposes:

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

Typical Network Implementation

This topic describes one possible network implementation of the Sterling Sensitive Data Capture Server along with the Sterling Web, Sterling Field Sales, Sterling Call Center, Sterling Store, and Sterling Distributed Order Management applications. The *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 Sterling Commerce applications perform the following roles:

- The Sterling Web (SW) application provides the e-tailer experience, such as catalog and product browsing, and shopping cart management.
- 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 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 four channels:
  - Internet-based (B2B or B2C) users interact with the Sterling Web application to browse items, create shopping carts, and then proceed to check out the cart.

- Internet-based users, such as sales representatives, generate complex sales quotes and then proceed to create the orders through the Field Sales 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 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.

Difference Between PCI Compliance and PA-DSS Validation

As a software vendor, Sterling Commerce's responsibility is to be Payment Card Industry (PCI) Payment Applications Data Security Standard (PA-DSS) Validated.

Sterling Commerce has performed an assessment and certification compliance review with an independent assessment firm to ensure that Sterling Commerce's 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 Sterling Commerce Applications

The Sterling Sensitive Data Capture Server (SSDCS), the service component used by Sterling Commerce 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 Web and Distributed Order Management applications have been architected to use the SSDCS so that they never capture, store, process, or transmit PAN. If you maintain this separation, you should be able to keep these applications 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.

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

The following security standards must be considered for proper implementation in a PCI-Compliant environment:

- "Remove Historical Credit Card Data (PA-DSS 1.1.4.a)"
- "Sensitive Authentication Data Requires Special Handling (PA-DSS 1.1.5.c)"
- "Purging of Cardholder Data (PA-DSS 2.1.a)"
- "Removal of Cryptographic Material (PA-DSS 2.7.a)"
- "Set Up Good Access Controls (PA-DSS 3.1.c and PA-DSS 3.2)"
- "Train and Monitor Administrative Personnel"
- "Key Management Roles and Responsibilities (PA-DSS 2.5)"
- "Log Settings Must Be Compliant (PA-DSS 4.2.b)"
- "PCI-Compliant Wireless Settings (PA-DSS 6.1.b and PA-DSS 6.2.b)"
- "Never Store Cardholder Data on Internet-Accessible Systems (PA-DSS 9.1.b)"
- "PCI-Compliant Delivery of Updates (PA-DSS 10.1)"
- "PCI-Compliant Remote Access (11.2 and 11.3.b)"
- "Data Transport Encryption (PA-DSS 12.1.b)"
- "PCI-Compliant Use of End User Messaging Technologies (PA-DSS 12.2.b)"
- "Nonconsole Administration (PA-DSS 13.1)"
- "Network Segmentation"
- "Maintain An Information Security Program"

Remove Historical Credit Card Data (PA-DSS 1.1.4.a)

PA-DSS 1.1.4.a 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 v1.2.

Customers who currently store sensitive authentication data in the associated Sterling Distributed Order Management or Sterling Web applications 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, Sterling recommends 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.

The Sterling Web and the Sterling Field Sales applications are new. As a result, there are no historical PANs to be removed.

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. Unfortunately, at Sterling Commerce we are unaware of any secure wipe tool or secure wipe procedure where you can securely replace a PAN without leaving residual traces in databases or where you can safely assure that all PAN occurrences are securely removed. As a result, there is a window of exposure during which your system will 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.

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

PA-DSS 1.1.5.c 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.a)

PA-DSS 2.1a 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 v1.2.

Key Management Roles and Responsibilities (PA-DSS 2.5)

PA-DSS 2.5 states that the payment application must 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 Web and Sterling Distributed Order Management applications to off load Primary Account Numbers to your credit vault server in exchange for a surrogate token.

Similarly, the Sterling Web and Sterling Distributed Order Management applications do not store encrypted PAN. As a result, the SSDCS and Sterling Commerce 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.a)

PA-DSS 2.7a 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 v1.2.

You must remove all cryptographic material that the Sterling Distributed Order Management and Sterling Web applications 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 Good Access Controls (PA-DSS 3.1.c and PA-DSS 3.2)

PA-DSS 3.1c and PA-DSS 3.2 state that the SSDCS:

- Does not require the use of default administrative accounts for payment application logins.
- Assigns secure authentication to default accounts, even if not used, and disables or does not use the accounts.
- Uses secure authentication for the payment application and the system, whenever possible.
- Describes how to create secure authentication to access the payment application, per PCI DSS Requirements 8.5.8 through 8.5.15.

The PCI DSS requires that access to all the 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 or process, with no generic group accounts used by more than one user or process. The following should be followed:

- Do not use administrative accounts for application logins. For example, do not use the SQL System Administrator account for application access to the database.
- Assign strong passwords to default accounts, even if they will not be used, and then disable the default accounts if they are not used.
- Assign strong application and system passwords whenever possible.
- Create PCI DSS-compliant complex passwords to access the payment application, per PCI Data Security Standards 8.5.8 through 8.5.15.
- Changing the out-of-the-box settings for unique user IDs and secure authentication will result in noncompliance with the PCI DSS.The Sterling Sensitive Data Capture Server is a simple tokenization proxy that does not have defined users or roles. As a result, the PA-DSS 3.1c and 3.2 requirements do not apply.

The SSDCS does not rely on application-level administrators to manage it. 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 runs.

For users, the PCI standard requires the following password complexity for compliance (often referred to as using “strong passwords”):

- Do not use group, shared, or generic user accounts (8.5.8).
- Passwords must be changed at least every 90 days (8.5.9).
- Passwords must contain at least 7 characters (8.5.10).
- Passwords must include both numeric and alphabetic characters (8.5.11).
- New passwords cannot be the same as the last 4 passwords (8.5.12).

Beyond uniqueness and password complexity, following are the PCI user account requirements:

- If an incorrect password is provided 6 times, the account should be locked out (8.5.13).
- Account lock-out duration should be at least 30 minutes, or until an administrator resets it (8.5.14).
- Sessions that are idle for more than 15 minutes should require re-entry of user name and password to reactivate the session (8.5.15).
- Control access through unique user names and PCI DSS-compliant complex passwords to any PCs or servers with payment applications, and to databases storing cardholder data.

To be PCI compliant, any applications or databases included in payment processing must also apply these account and password criteria. Sterling Commerce, as tested in its PA-DSS audit, meets or exceeds these requirements.

Sterling Sensitive Data Capture Server must require unique user names and complex passwords for all administrative access and for all access to cardholder data.

Note: These password controls are not intended for employees who have access to only one card number at a time to facilitate a single transaction. These controls are applicable to employees with

administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.

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.

Log Settings Must Be Compliant (PA-DSS 4.2.b)

PA-DSS 4.2b 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.

Note: With respect to PCI DSS 10.2.7, except for the creation of the application logs for logging and auditing purposes, 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 Sensitive Data Capture Server: 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 (http://en.wikipedia.org/wiki/Open_Source_Tripwire). The discussion of the use and configuration, or selection of the external monitoring tools is beyond the scope of this document.

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

PA-DSS 6.1 and PA-DSS 6.2b 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.b)

PA-DSS 9.1b 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 Delivery of Updates (PA-DSS 10.1)

PA-DSS 10.1 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, Sterling Commerce 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 patch that helps protect the Sterling Sensitive Data Capture Server against a specific, new vulnerability. We attempt to publish a patch within 30 days of a critical vulnerability being identified. We then contact vendors and dealers to encourage them to install the patch. Typically, merchants are expected to respond quickly to and install the available patches 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.

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

PCI-Compliant Remote Access (11.2 and 11.3.b)

PA-DSS 11.2 and 11.3b state that payment applications must use two-factor authentication if the payment application may be accessed remotely. These factors are:

- User ID and password
- An additional authentication item, such as a token

The Sterling Sensitive Data Capture Server is designed to run in your data center either in a DMZ or a trusted network. Administrators in the 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. Administrators who connect to the Sterling Sensitive

Data Capture Server remotely must do so within a Virtual Private Network. Access must be authenticated using a two-factor authentication mechanism (username/password and an additional authentication item, such as a token or certificate).

Administrators who access the server remotely should adhere to the following guidelines:

- Remote access passwords are changed every 90 days.
- A minimum password length of at least seven characters is required.
- Passwords containing both numeric and alphabetic characters are required.
- New passwords that are the same as any of the last four are not allowed.
- Repeated access attempts are blocked by locking out the user ID after not more than six attempts.
- The lockout duration is set to a minimum of 30 minutes or until the administrator enables the user ID.
- If a session has been idle for more than 15 minutes, the user must re-enter the password to re-activate the terminal.
- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication and complex passwords for logins, according to PCI DSS Requirements 8.1, 8.3, and 8.5.8 - 8.5.15.
- Enable encrypted data transmission according to PCI DSS Requirement 4.1:
  - Strong encryption must be used during data transmission.
  - The server can support the latest patched versions of SSL.
  - HTTPS appears as a part of the browser Universal Record Locator .
  - No cardholder data is required when HTTPS does not appear in the URL.
  - Transactions were observed to encrypt cardholder data during transit.
  - Only trusted SSL/TLS keys and certificates are accepted.
  - Proper encryption strength was verified to be implemented for the encryption methodology in use.
  - For wireless networks transmitting cardholder data or connected to the cardholder data environment, guidance on industry best practices (for example, IEEE 802.11i) is provided to implement strong encryption for authentication and transmission.
- Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13.
- Configure the system so a remote user must establish a Virtual Private Network (VPN) connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer passwords for authorized reseller and integrator personnel.
- Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.

The Sterling Sensitive Data Capture Server does not require vendor remote access accounts. As a result, you should ensure that vendor accounts are not created on the system. The Sterling Sensitive Data Capture Server does not require specialized remote access software such as Virtual Networking Computing (VNC),

Remote Desktop Protocol (RDP), or Symantec pcAnywhere. You should consider disabling these services for security hardening.

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).

Data Transport Encryption (PA-DSS 12.1.b)

PA-DSS 12.1.b 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 12.2.b)

PA-DSS 12.2.b 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 13.1)

PA-DSS 13.1 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 Windows protocol that is tunneled through SSH. By default, X Windows 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 14.1)

PA-DSS 14.1 states that the payment application vendor must develop, maintain, and disseminate a *PA-DSS Implementation Guide*(s) for customers, resellers, and integrators.

The *PA-DSS Implementation Guide* (“IG”) will be reviewed on a yearly basis, whenever the underlying application changes, or whenever the PA-DSS requirements change. Sterling Commerce will distribute this guide to new customers in the product documentation DVD. In addition, Sterling Commerce will provide updates through the Online Documentation Library at the Sterling Commerce Customer Center at the following URL:

https://cn.sterlingcommerce.com/login.jsp

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 Sterling Commerce 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.

Application System Configuration

Refer to the *Selling and Fulfillment Foundation: Installation 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 Sensitive Data Capture Server: 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. This is documented in the *Sterling Sensitive Data Capture Server: Configuration 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.

Index

R

S

T

U

V

W