Sterling Store Associate Mobile

PA-DSS Implementation Guide

Version 3.2.02

Sterling Store Associate Mobile

PA-DSS Implementation Guide

Version 3.2.02

Note
Before using this information and the product it supports, read the information in "Notices" on page 23.

Contents

Chapter 1. Roadmap: Using the PA-DSS and Sterling Store Associate Mobile Documentation Guides

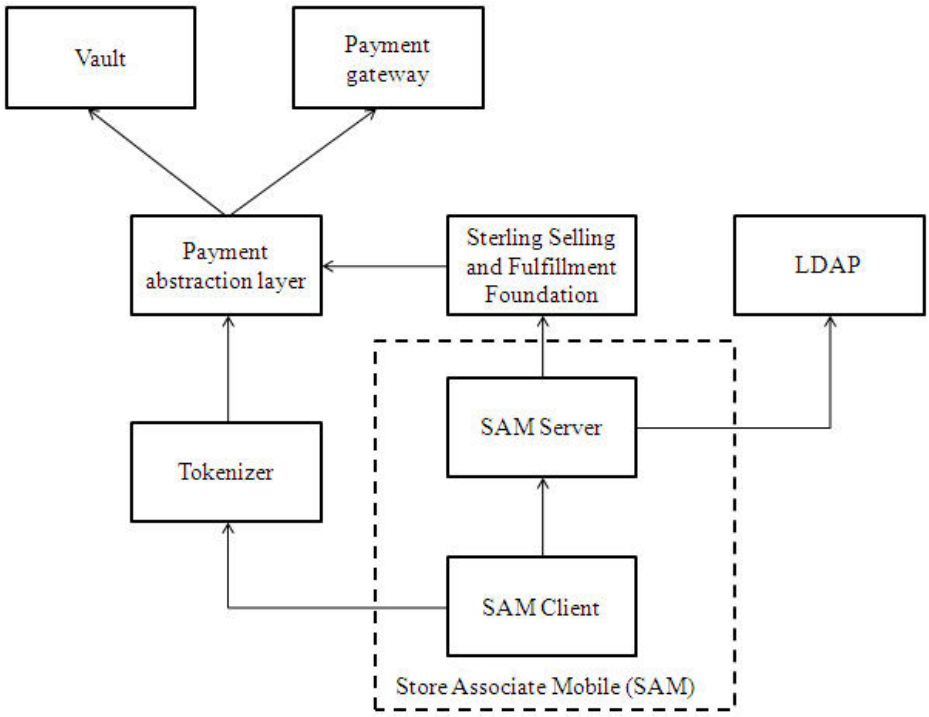
This document provides guidance on how to implement the IBM® Sterling Store Associate Mobile (SAM) application for secure credit card capture and protection, in accordance with the Payment Application Data Security Standard (PA-DSS) and the Payment Card Industry Data Security Standard (PCI DSS).

Sterling Store Associate Mobile Architecture

Store associates can use SAM to access and use information on product content and inventory availability to handle customer inquiries anytime and anywhere in a retail store. The application can also give store associates the ability to save the sale handle out-of-stock situations in an efficient manner.

As depicted in the diagram below the SAM is a client/server application where the client component runs on iPod and iPhone devices and the server-side component runs on a J2EE application server. The SAM server-side component is integrated with the IBM Sterling Selling and Fulfillment Foundation application. When store associates performs tasks such as viewing order or inventory availability, or capturing orders on the iPod Touch device, the client component sends the requests to the server side component which in turn forwards the requests to the Sterling Selling and Fulfillment Foundation application for processing. Either Release 8.5 or Release 9.1 or Release 9.2 can be used.

When the store associate captures a credit card number or Primary Account Number (PAN) on the iPod Touch device, the SAM client component sends the PAN to a “tokenizer”. The tokenizer can be the Sterling Sensitive Data Capture Server (SSDCS) if SAM is integrated to Release 9.1 or Release 9.2. Alternatively, SAM could be integrated to a custom-built tokenizer.



At a high level, implementing the Sterling Store Associate Mobile application involves the following steps:

1. Install the server component of Sterling Store Associate Mobile application from the installation CD.
2. Install the Sterling Selling and Fulfillment Foundation application from the installation CD. Sterling Store Associate Mobile works with Sterling Selling and Fulfillment Foundation, Release 8.5 or 9.1 or 9.2.
3. Integrate the SAM server component to the Sterling Selling and Fulfillment Foundation application, and establishing a trust relationship.
4. Integrate the SAM server component to an external authentication framework such as LDAP.
5. Provide a tokenizer service. As mentioned above, you can either provide your own tokenizer service or use the IBM Sterling Sensitive Data Capture Server (SSDCS) if you are using Sterling Selling and Fulfillment Foundation, Release 9.2.
6. Integrate the SAM client component to the tokenizer service.
7. Provide a payment abstraction layer.
8. Integrate the Sterling Selling and Fulfillment Foundation application and the tokenizer to the payment abstraction layer.
9. Integrate the payment abstraction layer to your credit card vault and payment gateway.

Sterling Store Associate Mobile works with the Sterling Selling and Fulfillment Foundation. For more information about installation, refer to the *Sterling Selling and Fulfillment Foundation: Installation Guide*. For more information about the application, refer to the *Sterling Store Associate Mobile: Application Guide*.

About the PA-DSS Implementation Guide

The PA-DSS Implementation Guide describes the steps that you must follow for your Sterling Store Associate Mobile installation to remain in compliance with the Payment Application - Data Security Standard (PA-DSS).

The information in this document is based on the PCI Security Standards Council (PCI SSC) PA-DSS program (version 2.0, dated October, 2010). It is recommended that you deploy Sterling Store Associate Mobile and its backend 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 Sterling Store Associate Mobile installations will not be PA-DSS compliant and the Sterling applications could be considered to be within PCI DSS auditing scope.

Sterling Store Associate Mobile, Release 3.2.02:

PA-DSS Implementation Guide Revision Information

Table 1. Revision Information

Revision Information	
Authors	Bernie Wong, Performance Engineering Director, Security Advisor Ninad Manelkar, Software Engineering Manager
Approving Authority	Steven Aulds, Director of Development and SaaS Operations, IBM Commerce
Revision Date	03/31/2011
Next Review Date	03/31/2012, or whenever the underlying application changes, or whenever the PA-DSS requirements change
Exclusions https://www.pcisecuritystandards.org/security_standards	Applies to all Engineering employees who develop or maintain the Sterling Store Associate Mobile application

Sterling Store Associate Mobile, Release 3.2.02: PA-DSS Implementation Guide Update History

Table 2. Update History

Name	Title	Date	Summary of Changes
Ninad Manelkar	Software Engineering Manager	03/01/2012	Reviewed for Release 3.2.02 and no changes required.

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.

Overview of the PA-DSS Implementation Guide

The Sterling Store Associate Mobile application enables store associates to select multiple payment methods and use a credit card reader to bill the customer for a purchase. The application calls an external tokenizer service 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. The Sterling Store Associate Mobile application, Release 3.2.02, 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

Additional details surrounding the PCI SSC and related security programs, such as PA-DSS and PCI DSS, are available from:

Sterling Store Associate Mobile Application Summary

Table 3. Application Summary

Application Feature	Description
Name	Sterling Store Associate Mobile
Application Version Number	3.2.02
Components of the Application, such as POS and Back Office	The Sterling Store Associate Mobile application captures credit card and other sensitive information. It calls a tokenizer service to convert the credit card into tokens for security. It sends the tokens to the Sterling Selling and Fulfillment Foundation application.
Credit Card Server(s)	The Sterling Store Associate Mobile application does not use credit card servers.

Table 3. Application Summary (continued)

Application Feature	Description
Other Required Third-Party Software	The Sterling Store Associate Mobile application requires the following software components: • Apple iPhone SDK • Linea Pro SDK: The Linea Pro SDK is used with the portable integrated barcode scanner and magnetic reader to read credit card information. Refer to the *Sterling Store Associate Mobile: Application Guide* for the current supported version numbers.
Setup	Components of the application, such as POS and Back Office. The Sterling Store Associate Mobile application is used to capture credit card information, tokenize the PAN using a tokenizer service, and send the token to the Sterling Selling and Fulfillment Foundation application. The Sterling Store Associate Mobile application installation and configuration steps are documented in the *Sterling Store Associate Mobile: Application Guide*.
Operating Systems	The Sterling Store Associate Mobile application is currently supported on the following operating systems: • Apple iPhone OS Refer to the *Sterling Store Associate Mobile: Application Guide* for the current supported version numbers.
Code Base, DB Engine	The Sterling Store Associate Mobile application does not use a database engine.
Application Description	Sterling Store Associate Mobile is an application that enables a store associate to search the catalog, view inventory availability in a store and other stores located within a specified radius, view item-related information such as item specifications, promotions, and related items, place an order, and perform backroom pick for customer orders. As part of placing an order, the Sterling Store Associate Mobile application captures PAN information, calls a tokenizer service to tokenize and store credit card and gift card numbers in a credit card vault. The token is sent to the Sterling Selling and Fulfillment Foundation application as part of the order so that the customer can be billed for the purchase.
Application Environment	The Sterling Store Associate Mobile application runs in the Internal or Trusted network since it is a service to internal users. Sterling Store Associate Mobile is a mobile application running in an iPhone OS environment on an iPhone or iPod Touch device. The Sterling Store Associate Mobile application does not use or rely on a database server.

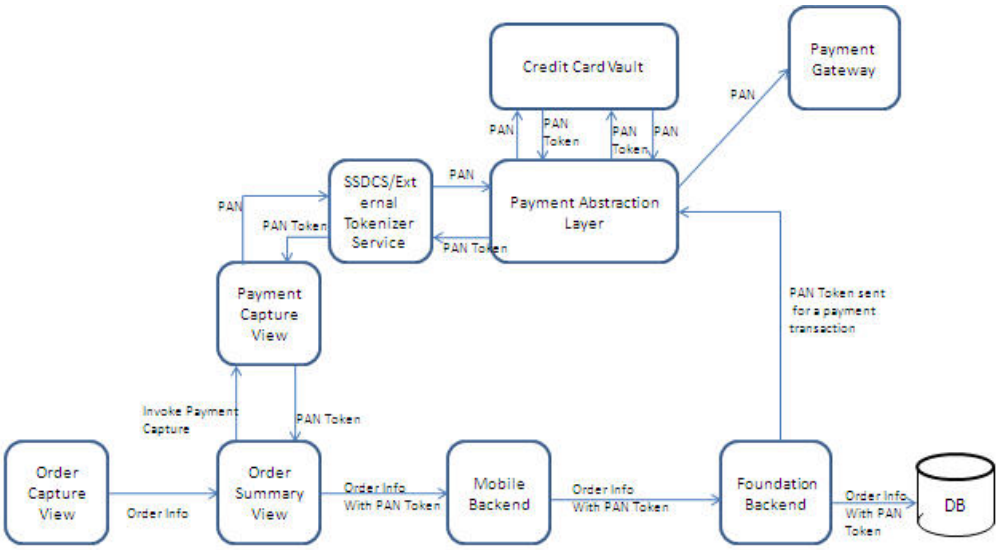
Table 3. Application Summary (continued)

Application Feature	Description
Application Target Clientele	The Sterling Store Associate Mobile application is used by organizations to handle out-of-stock situations more efficiently by enabling the store associate to obtain real-time information on product inventory availability directly from the store associate's mobile device, and then guiding the customer on how to best obtain the product to improve responsiveness to the customer's need. The Sterling Store Associate Mobile application enables the store associate to search the catalog, scan the barcode to get the details of an item, view inventory availability in a store and its nearby stores within a specific radius, place an order for a consumer, use the credit card reader to bill the consumer for a purchase, and perform backroom pick for customer orders.
Description of Versioning Methodology	We release major versions of the Sterling Store Associate Mobile application on a regular basis. Version numbering is denoted in the X.Y.ZZ format, for example, 3.0.07 where X is the major version number, Y is the minor version number, and ZZ is a patch version number. Major changes are officially scheduled software releases that introduce new features as a result of roadmap development occurring every 6-12 months on an average. Significant enhancements such as integration with Magnetic Card Readers that affect PA-DSS would typically happen in a major release and would be denoted by updating the X component in the version number. Minor changes are feature enhancements that are released as needed and typically occur every 2-6 months. Minor changes are typically denoted by updating the Y component in the version number. These could include addition of new screens, including payment-related screens. We will ensure, at a minimum, that changes to payment-related screens are tracked as a minor change. Patch changes are changes released as needed in response to customer-reported software failure or enhancement request. Patch changes are typically denoted by updating the ZZ component in the version number. These equate to rollups, update releases, hotfixes or patches, or customer-directed minor enhancements. Changes that qualify for PA-DSS review will NOT be released as a patch change.

Data Flow Diagram Depicting the Order Capture Data Flow

This section describes the flow of the Primary Account Number (PAN) for the Sterling Store Associate Mobile application.

The following data flow diagram illustrates the order capture function:



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

First Path:

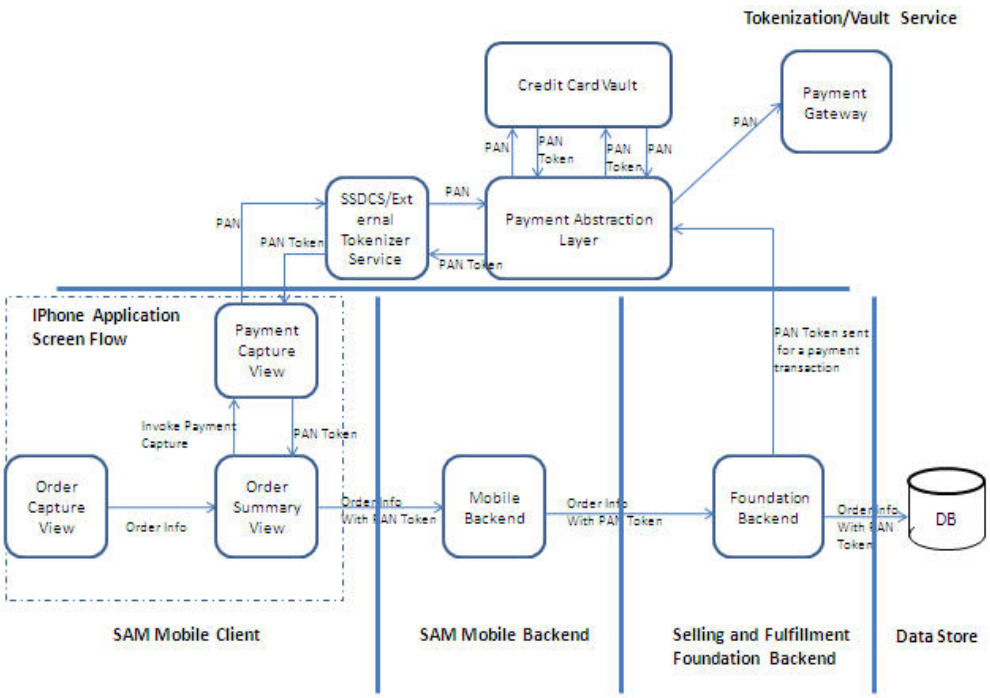
1. The Store Associate Mobile application payment capture screen is used to capture PAN.
2. The PAN information is then sent to the customer's tokenizer service which in turn forwards the PAN to the customer's credit card vault for tokenization.
3. The PAN is stored in the credit card vault.
4. A token is returned to the payment capture screen.

Second Path:

1. The token from the first path and the order information are gathered during the order capture process and sent to the Sterling Selling and Fulfillment Foundation application that operates as an order store.

The key point is that the second path does not transmit sensitive PAN information.

The following data flow diagram shows the Order Capture Data Flow data flow between components:



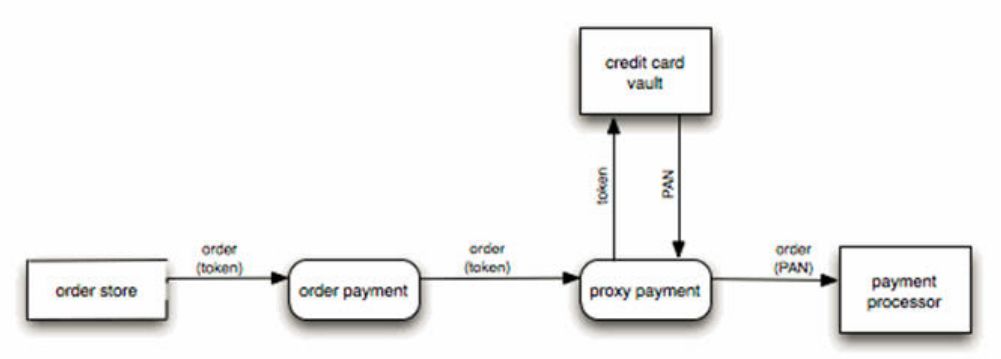
In terms of software partitioning, the PAN is captured in the browser along with the order information, as follows:

1. From the browser, the PAN information is sent to a tokenizer service 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 Sterling Selling and Fulfillment Foundation applications contains only the order information and PAN token, and 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 Sterling Selling and Fulfillment Foundation applications do not touch PAN. This means that these applications may be kept outside of the PCI DSS auditing scope.

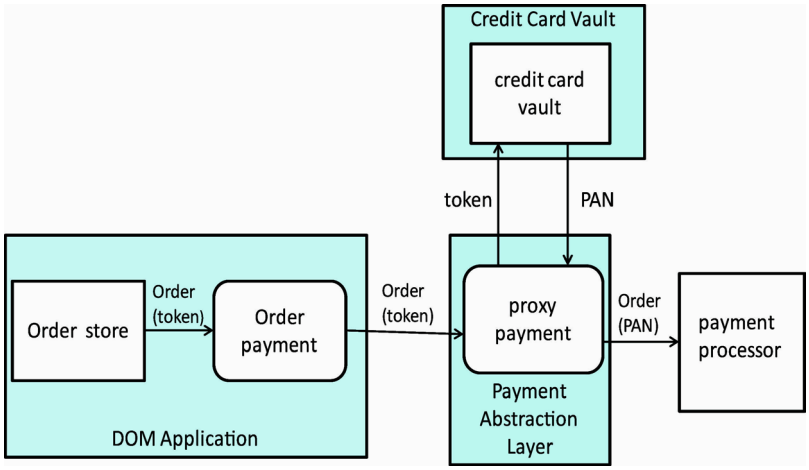
The following diagram illustrates a Payment Processing Transaction.



In this 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.



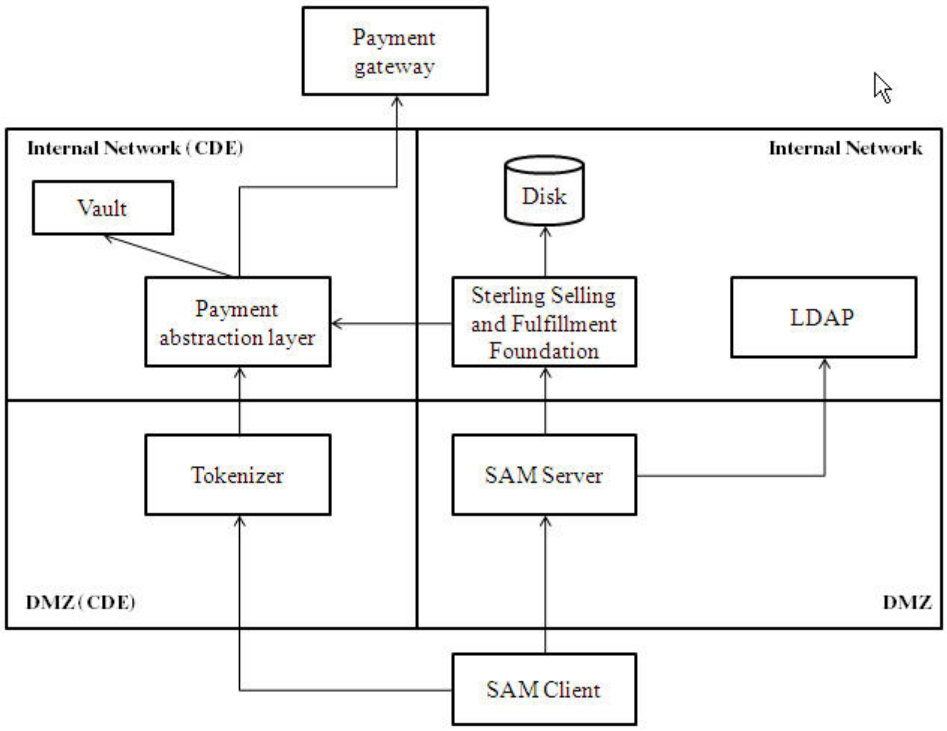
In this illustration, the task of detokenization is delegated to a component called the Payment Abstraction Layer (PAL). This is a customer-provided component. This partitioning approach serves two critical purposes:

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

Typical Network Implementation

This topic describes the network implementation of the Sterling Store Associate Mobile application along with the Sterling Selling and Fulfillment Foundation application.

The following diagram illustrates a typical network implementation:



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

- The Sterling Store Associate Mobile application provides the store associate of the organization with better access and use of information on product content and inventory availability to handle customer inquiries anytime and anywhere in a retail store. It provides the store associates the ability to save the sale and satisfy their customer with the power of inventory visibility, fulfillment, and status tracking and reporting, at their fingertips by the use of a mobile device. This can enable a retail business to save the sale when faced with an in-store stock-out and the opportunity to reserve inventory for in-store pickup.
- The Sterling Store Associate Server Side Component acts as a conduit for the Sterling Store Associate Mobile application to interface with the Sterling Selling and Fulfillment Foundation application.
- The Sterling Selling and Fulfillment Foundation provides order fulfillment functionality, such as performing payment authorization, picking fulfillment channels, and so on.

As the previous illustration shows, the Store Associate Backend and the Sterling Selling and Fulfillment Foundation applications are deployed separately in the Internal Trusted Network Zone.

The tokenizer service is part of the PCI Cardholder Internal Network. Sterling Cardholder data is kept away from the database and the tokenizer service. Because the tokenizer service performs all the tokenization and detokenization requests for payment processing, it can be monitored and securely protected. The Sterling Store Associate Mobile application captures and uses the tokenizer service to tokenize the PAN while the Sterling Selling and Fulfillment Foundation 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, it is our responsibility is to be Payment Card Industry (PCI) Payment Applications Data Security Standard (PA-DSS) Validated.

We have performed an assessment and certification compliance review with an independent assessment firm to ensure that the 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 Store Associate Mobile Applications

Sterling Store Associate Mobile is an application that merchants can use to enhance the shopping experience and to assist in the order checkout process for their shopping consumers. The Sterling Store Associate Mobile application relies on being able to offload sensitive PAN to the merchant's credit card vault through tokenization. The SAM application is in the process of being validated to the PCI PA-DSS security standards. The merchant is expected to follow the instructions provided in this guide to ensure that Sterling Store Associate Mobile is implemented in such a manner that the merchant achieves PCI PA-DSS compliance.

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.
3. **Protect Cardholder Data**

   Protect stored data.

4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. **Maintain a Vulnerability Management Program**

   Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. **Implement Strong Access Control Measures**

   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.
10. **Regularly Monitor and Test Networks**

    Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. **Maintain an Information Security Policy**

    Maintain a policy that addresses information security.

Chapter 2. 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)

PA-DSS Requirement 1.1.4 states that sensitive authentication data stored by previous payment application versions have to be deleted.

The Sterling Store Associate Mobile application does not store historical credit card data. Therefore, there is no historical credit card information to remove from the Sterling Store Associate Mobile application, as required by PA-DSS Requirement 1.1.4.

Sterling Store Associate Mobile application captures credit card information as part of its order capture process. After capture, the Sterling Store Associate Mobile application sends the PAN to the customer-provided tokenizer service. The tokenizer service returns a PAN token back to the order capture process. After the tokenization process is completed, the PAN is destroyed. The rest of the order

capture process only uses the PAN token. The order sent to the order store (Sterling Selling and Fulfillment Foundation application) only processes tokens.

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 Sterling Store Associate Mobile application because the Sterling Store Associate Mobile application only captures the PAN. The application specifically does not capture or use the sensitive authentication data (For example, full magnetic stripe data, CAV2/CVC2/CVV2/CID, or PIN/PIN Block).

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 the payment application stores cardholder data.

This requirement does not apply to the Sterling Store Associate Mobile application because it does not store cardholder data. Therefore, there is no data to be purged, as required by PA-DSS v2.0.

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

PA-DSS 2.5 and PA-DSS 2.6 states that the payment application must implement key management processes and cryptographic keys used for encryption of cardholder data against disclosure and misuse.

This requirement does not apply to Sterling Store Associate Mobile because the application neither stores cardholder data nor does it provide any configurability that would allow a merchant to store cardholder data.

Sterling Store Associate Mobile collects PAN on behalf of an order capture process. The PAN is sent to the customer's tokenizer service. The tokenizer service returns a PAN token back to the order capture process. After the tokenization process is completed, the PAN is deleted. Sterling Store Associate Mobile ensures that only the token is sent to the Sterling Selling and Fulfillment Foundation.

As a result, the Sterling Store Associate Mobile application does not use cryptography to encrypt PAN.

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.

This requirement does not apply to Sterling Store Associate Mobile application because the application does not use cryptography to encrypt PAN as the PAN details are not stored. Also, the application only processes and transmits tokens. As a result, there is no cryptographic data to be securely removed as required by PA-DSS v2.0.

You must remove all cryptographic material that the Sterling Selling and Fulfillment Foundation application used to encrypt PAN. If you are upgrading from an earlier version of this application, 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 2.0, Requirement 3.1c states that "payment applications must facilitate use of unique user IDs and secure authentication for all administrative access and for all access to cardholder data."

This requirement is not applicable to the Sterling Store Associate Mobile application because neither the client nor the server component implemented an administrative interface. The server component is maintained and administered through either the operating system shell or through the administrative console of the application server.

PA-DSS 2.0, Requirement 3.2 states that "access to PCs, servers, and databases with payment applications must require a unique user ID and secure authentication." Merchants and their resellers or integrators are advised to follow these guidelines:

- Avoid using default administrative accounts to administer or maintain the Sterling Store Associate Mobile application – for example, do not use the "system" user in administering IBM WebSphere®.
- Assign secure authentication to these default accounts (even if they are not being used), and then disable or do not use the accounts.
- Assign secure authentication to the application server and systems whenever possible.
- Create PCI DSS-compliant secure authentication to access the application server and operating system, per PCI DSS Requirements 8.5.8 through 8.5.15
- Changing "out of the box" installation settings for unique user IDs and secure authentication will result in non- compliance with PCI DSS. The Sterling Store Associate Mobile application 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.

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 on. 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 occurs because of unethical personnel. Therefore, pay special attention to the people you trust your administrative site with and to those whom you allow to view full decrypted and unmasked payment information.

Sterling Store Associate Mobile is a client-side application. There is no administrative role for the client-side application. The administration is managed by the Sterling Selling and Fulfillment Foundation application. Also, there may be administrative roles to configure the tokenizer service. It is the customer's responsibility to train their administrative personnel accordingly for management and monitoring of such applications.

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 non-compliance with PCI DSS.

The “out-of-the-box” default installation of the Sterling Store Associate Mobile application enables logging on the server-side component. As noted above, merchants who disable logging will result in non-compliance with PCI DSS.

Out-of-the-box, the Sterling Store Associate Mobile Application 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 Store Associate Mobile: Properties Guide*.

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 Store Associate Mobile application uses 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.

This is not applicable to Sterling Store Associate Mobile because this application does not store cardholder data. Sterling Store Associate Mobile captures PAN on behalf of an order capture process. That PAN is sent to the customer's tokenizer service. The tokenizer service returns a PAN token back to the order capture process. After the tokenization process is completed, the PAN is deleted. Sterling Store Associate Mobile ensures that only the token is sent to the Sterling Selling and Fulfillment Foundation.

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, we keep 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 Store Associate Mobile application 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 only available through Apple App Store. Sterling Store Associate Mobile application has a unique identifier. Only authorized personnel can upload the application by the same unique identifier.

The only way to upload a patch is to upload the entire iPhone application. Once you upload the full application that includes the fix (for which a "patch" was required), Apple automatically notifies all the iPhone/iPod users that an updated version is available. It is the user's choice to update to the latest version. But when the user makes the choice to update to the latest version, we ensure that the correct targeted version is downloaded due to the single conduit availability through the Apple App Store.

Using Two-Factor Authentication (PA-DSS 10.2)

PA-DSS 10.2 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 Store Associate Mobile application is a client application. It does not have any administrative capabilities. The administrative functionality is handled by the Sterling Selling and Fulfillment Foundation application.

The Sterling Store Associate Mobile application does not require vendor remote access accounts. As a result, you should ensure that vendor accounts are not created on the system.

The Sterling Store Associate Mobile application 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 Store Associate Mobile application 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).

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

PA-DSS 5.4 states that the payment application must only use or require use of necessary and secure services, protocols, daemons, components, and dependent software and hardware, including those provided by third parties, for any functionality of the payment application (for example, if NetBIOS, file- sharing, Telnet, FTP, etc., are required by the application, they are secured via SSH, S-FTP, SSL, IPSec, or other technology).

The Sterling Store Associate Mobile Application is an iPhone application that makes requests external tokenizer or Sterling Secure Data Capture Server(SSDCS). The Sterling Store Associate Mobile Application also sends the order information gathered during the order capture process, to the Sterling Selling and Fulfillment Foundation application that operates as an order store. The only service it requires is access to the HTTPS port.

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

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

PA-DSS 10.3.2 states that if vendors, resellers/integrators, or customers can access customers' payment applications remotely, the remote access must be implemented securely.

Customers who allow vendors, resellers or integrators to access the SAM remotely should adhere to the following guidelines:

- 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 (See PA-DSS Requirements 3.1.1 through 3.1.10)
- Enable encrypted data transmission according to PA-DSS Requirement 12.1
- Enable account lockout after a certain number of failed login attempts (See PA-DSS Requirement 3.1.8)
- 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 to authorized reseller/integrator personnel.
- Establish customer passwords according to PA-DSS Requirements 3.1.1through 3.1.10.

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.

The Sterling Store Associate Mobile application uses the following two communication paths

- the path from the Sterling Store Associate Mobile client component to the server component and
- the path from the Sterling Store Associate Mobile client component to the customer's tokenizer service

The communication configuration is made on the server and on each individual mobile device. On the server side, the administrator sets two parameters:

- `yfs.sam.PADSS.disable` - The default value of this property is blank and hence ensures mandatory communication to the external tokenizer/SSDCS server.e
- `yfs.sam.PADSSServerURL= <hostname, virtual IP or IP of the customer's tokenizer service>`

On the client side, each user sets the URL of the Sterling Store Associate Mobile application server side.

For production, the tokenizer URL and the URL of the Sterling Store Associate Mobile application server component should be set to use HTTPS.

The communication end points are specified in two different places. First, after installing the client component to the mobile device, the user, who could be a tester or a store associate, enters the URL of the application server. The Sterling Store Associate Mobile application client issues a warning if the user enters the URL with the HTTP protocol.

On the server component, if the yfs.sam.PADSS.disable in the INSTALL_DIR/properties/yfs.properties_ssa_ext property file is set to blank, ensuring mandatory communication to the external tokenizer/SSDCS server.. Similarly, the server component ensures the communication path from the client component to the customer tokenizer is under HTTPS.

Refer to the topic “Data Flow Diagram Depicting the Order Capture Data Flow” on page 6 for an understanding of the encrypted data flow associated with the Sterling Store Associate Mobile application.

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.

This requirement does not apply to the Sterling Store Associate Mobile application because the application does not use end-user messaging technology, such as e-mail, instant messaging, and chat to transmit PAN.

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.

Non-console administration access to the server-side component of the Sterling Store Associate Mobile application must only be made secure tunneling protocols such as a VPN or SSH. There is no administration access to the client component of the Sterling Store Associate Mobile application.

The Sterling Store Associate Mobile application does not require the use of 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 will be reviewed on a yearly basis, whenever the underlying application changes, or whenever the PA-DSS requirements change. You can find the updated documentation in the following link: http://www.ibm.com/support/docview.wss?uid=swg27023854

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 “Data Flow Diagram Depicting the Order Capture Data Flow” on page 6 for an understanding of the flow of encrypted data associated with the Sterling Store Associate Mobile application.

In the illustration in the topic “Typical Network Implementation” on page 9, PAN information from Internal Mobile Application users flows to an internal tokenizer service, which is in an internal cardholder data network for tokenization.

Tokens are used only in the Sterling Store Associate Mobile applications in the non-cardholder 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.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© IBM 2012. Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2012.

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.

Printed in USA