Merchant Link, LLC

Payment Application Data Security Standard (PA-DSS)

Partner Implementation Guide (Doc# 26-PTR000395)

Version 1.1 February 12, 2016

The information contained herein is provided “As Is” without warranty of any kind, express or implied including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. There is no warranty that the information or the use thereof does not infringe a patent, trademark, copyright, or trade secret.

Merchant Link, LLC, shall not be liable for any direct, special, incidental, or consequential damages resulting from the use of any information contained herein, whether resulting from breach of contract, breach of warranty, negligence, or otherwise, even if Merchant Link, LLC has been advised of the possibility of such damages. Merchant Link reserves the right to make changes to the information contained herein at any time without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Merchant Link, LLC

Merchant Link

Table of Contents

Contents

1 Readership, Distribution and Updates 3
2 Introduction 3
3 Cardholder Data Security Standards Overview 4
4 Benefits of the Merchant Link Solution 5
5 POSLynx220 and PAX Terminal Versioning 6
6 Data Security Standards Stakeholders 7
7 PA-DSS Requirements – POSLynx220 Specifics 8
8 TransNet on POSLynx - Implementation Considerations 22
9 Reference Links 24

1 Readership, Distribution and Updates

Merchant Link will distribute this guide to Partners that are reselling or intend to resell POSLynx220™ payment routers running Merchant Link's TransNet™ payment engine to their clients. The guide may also be sent directly to customers in the rare cases, where customers purchase this product directly from Merchant Link for payment applications. This guide is intended for Merchant Link Partners and their personnel and covers PA-DSS v1.2 requirements for the TransNet v2.12 release of the POSLynx family of devices. The guide will not necessarily be sent to POSLynx220 customers that do not run payment/financial transactions through their device(s).

Guide updates will always follow major new functionality releases and will generally be published upon any change to the TransNet™ application software that could affect security elements described in this guide. In these cases, a new version of the guide may be published and distributed or, in certain cases, only an addendum will be produced and distributed. Notices of new guide publication and/or updates will be sent to current Partners and the guides will be made available on Merchant Link's website and Partner Support Wiki.

2 Introduction

Cardholder data security is among the most critical issues facing today's retail payment industry. In recent years, the benefits of using internet protocol (IP) networks for transaction processing have become widely recognized, and most retailers use or plan to use the Internet in some aspect of their business, for transaction processing or other tasks such as ecommerce websites or inventory management. With this increase in Internet usage has come a growing awareness of the risks involved in using the public Internet to transmit consumer cardholder data.

In response, credit card companies have proactively implemented two key standards for securing cardholder data: the Payment Card Industry Data Security Standard (PCI DSS) and Payment Application - Data Security Standard (PA-DSS). These standards are designed to protect the consumer, while safeguarding the merchant and acquirer from liability.

Merchant Link has designed its payment applications and supporting products to meet and exceed each of these standards both today and in the future. Our approach to payments encrypts and secures card number and expiry date for the time between authorization and settlement. During this time, no access to this data is allows by any means, and after the settlement with the processor, no data remains anywhere in the system.

The products, which include the POSLynx220™ payment router, PAX Terminals, TransNet™ payment engine and NetVu™ management server, deliver the industry's most comprehensive approach to cardholder data security by housing the payment application on a secure router and maintaining PCI and PA-DSS compliance on an ongoing basis through alerts and updates.

3 Cardholder Data Security Standards Overview

In 2001, Visa® introduced the Cardholder Information Security Program (CISP), requiring compliance by all entities that store, process or transmit Visa cardholder data. MasterCard® soon followed suit with the Site Data Protection Plan (SDP).

Today, the industry has evolved to one common standard, which is endorsed by all card companies, called the Payment Card Industry Data Security Standard (PCI DSS). Merchants have a responsibility to understand their compliance requirements.

The rising incidence of cardholder data theft results in financial losses and a compromised reputation for the merchant, as well as inconvenience and personal loss to consumers. The sizeable fines levied by the card associations in the event of cardholder security breaches can have a significant effect on the merchant's bottom line.

3.1 Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a set of 12 best practices for entities that receive, store or transmit payment information. This means that they apply, for example, to merchants and service providers (like gateways and processing companies), but not to software/application providers. A separate program that was called the Payment Application Best Practices (PABP) and is now called Payment Application – Data Security Standard, applies to software/application providers. This distinction is an important one, because while PABP compliant software can offer merchants peace of mind, they have the additional obligation to demonstrate compliance with PCI DSS according to the applicable assessment program. As a general rule, merchants should deal with vendors and service providers who, like Merchant Link, demonstrate PCI and/or PA-DSS compliance.

PCI DSS requirements differ by type of merchant. To understand your PCI compliance obligations, visit https://www.pcisecuritystandards.org

3.2 Payment Application Data Security Standard (PA-DSS)

The PA-DSS standards are a voluntary set of guidelines that address the design and implementation of payment processing software. These guidelines address the risks associated with the storage of full magnetic stripe data or CVV2 values after authorization by payment applications. In February 2005, the PABP guidelines for software/application providers were aligned with the PCI DSS standards for merchants. This move makes it easier for merchants to understand the relationship between the software they use and their own compliance responsibilities.

Subsequently, in late 2008, the PABP standard was transferred from Visa to the PCI Security Standards Council. For more information on PA-DSS requirements, visit https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

Software vendors (developers of applications specifically for credit card transactions that store, process or transmit cardholder data as part of authorization or settlement) need to create a Report on Validation to validate that their application(s) comply with PA-DSS requirements. As the PA-DSS Requirements document states, "Secure payment applications, when implemented in a PCI DSS compliant environment will minimize the potential for security for security breaches leading to compromises of full magnetic stripe

data, card validation codes and values (CAV2, CID, CVC2 CVV2), PINs and PIN blocks, and the damaging fraud resulting from these breaches."

An approved list of PABP validated applications can be found at the following site: http://usa.visa.com/download/merchants/validated_payment_applications.pdf and an approved list applications validated against PA-DSS standards can be found at the following site: https://www.pcisecuritystandards.org/security_standards/vpa/

4 Benefits of the Merchant Link Solution

Together with our NetVu deployment and management server, Merchant Link offers the most comprehensive and secure non-PC based payment engine in the industry delivering the following benefits to merchants:

4.1 Industry Leading Data Security Approach

Merchant Link's solution leverages the proven POSLynx220 and PAX S80/S90 hardware to provide a safe location for the TransNet payment application. By removing the payment application from the PC and onto a more secure, proprietary device, cardholder data is less vulnerable. TransNet has been designed to meet and exceed relevant security standards and offers the industry's most comprehensive approach to securing cardholder data.

Merchant Links's innovative approach to security enforces PCI standards directly, without weeding through a multitude of options that could break PCI compliance should the wrong choice be made, say, in setting up the password requirements or virus application. This simplifies the deployment and management process for Merchant Link Partners, as detailed within this guide.

4.2 Leverage PCI and PA-DSS Requirements

Merchant Link solutions allow Partners to embrace PCI and PA-DSS questions and requirements from their customers, rather than responding with uncertainty, as is often the case. Knowing that the solution meets and exceeds the relevant data security standards, PCI DSS and PA-DSS, Merchant Link Partners can leverage cardholder security to gain a competitive edge.

Unlike many other solutions, Merchant Link's technology is automatically updated whenever standards change, working in the background to ensure the merchant is always compliant. This feature allows the merchant to focus on his core activities, knowing their systems are compliant.

4.3 Remote Monitoring and Management

For Partners that support merchants (network providers, ISOs, dealers), NetVu facilitates turnkey deployment and allows for remote problem determination, eliminating finger pointing between suppliers. In addition, NetVu provides a simple means of monitoring and managing field devices after deployment.

4.4 Enhanced Reliability and Integration Features

Merchant Link's solution is designed with the needs of the merchant in mind. Merchants requiring the lowest upfront and life-cycle costs on a manageable yet secure payment terminal will look to the PAX S80 or S90 running Merchant Link's TransNet Payment engine as their ideal solution.

Merchants requiring an integrated payments approach will move to the POSLynx220, which allows for the integration of multiple store peripherals, ensuring their solution continues to grow and scale in the future. Features such as automatic dial back-up and the additional serial/dial ports on the POSLynx220 ensure maximum uptime and redundancy in case of failure.

Merchant Link's innovative approach to security enforces PCI standards directly, without weeding through a multitude of options that could break PCI compliance should the wrong choice be made, say, in setting up the password requirements or virus application. This simplifies the deployment and management process for Merchant Link Partners, as detailed within this guide.

4.5 Transaction Reporting and Fraud Alerts

Growing card fraud has consumers spending more time reviewing their card statements. This inevitably requires the merchant to answer questions on particular charges the client may no longer remember that might have taken place month ago.

The merchant also has to be more diligent in reviewing their own statements, if available quickly, to spot fraud that may be chargeable to them.

Merchant Link has a comprehensive service available on both all platforms that allows partners to offer merchants the ability to stay on top of this growing problem.

MerchantVu™ provides detailed reporting on a store or groups of stores to research customer requests quickly and accurately. It also allows the Merchant to choose specific alerts to send to the Partner or Merchant, such as manual transactions, large refunds, or other potential fraudulent activities.

5 POSLynx220 and PAX Terminal Versioning

Merchant Link's v2.08, v2.09, v2.10 and v2.11 TransNet releases were only available on the POSLynx220 platform. These releases have similar methods of access, use the same core application processes and have full use of the onboard router and firewall. Router features common to these versions include firewall and port filtering for security and automatic dial back-up for solution reliability. The POSLynx v2.08 release cannot create transactions; only convert transactions from existing payment devices, changing the protocol appropriate to the target host(s). The POSLynx220 v2.08 and v2.09 customers should be planning to upgrade to newer versions in the near future to ensure compliance with the latest PCI requirements.

POSLynx220 versions 2.10, 2.11 and 2.12 act much more like a POS payment application and, once provided with card number, expiry date and other data (as required by processor), construct and process the transaction over an IP network. These TransNet versions allow the POSLynx220 to be used locally in a store environment or remotely,

connecting various stores as a mini switch. In addition to integrating more models of ECR and POS Systems, Virtual Terminal and eCommerce support have been upgraded and tracking of both electronic payments and cash payments (where supported) can be reported on using Merchant Link's MerchantVu server.

More complete descriptions of all Merchant Link applications and their PABP and PA-DSS validations are provided in previous Partner Implementation Guide releases.

Note: *For the remainder of this guide, 'POSLynx', 'POSLynx220' are used to denote POSLynx220 running TransNet. Unless specifically stated otherwise, 'TransNet', 'TransNet release', 'TransNet application' and similar phrases will be used to denote Merchant Link's TransNet v2.12 payment engine application.*

6 Data Security Standards Stakeholders

6.1 Payment Application Providers

As part of the PA-DSS Program requirements, application/software providers like Merchant Link must provide documentation to assist their Partners.

Confidential (doc# 26-PTR000395) Page 7 understanding how the POSLynx220 with NetVu and TransNet help facilitate PCI compliance obligations of merchants. This Guide is intended to provide this information in a simple and straightforward way.

IMPORTANT NOTE: Merchants, processors, and other parties have a direct responsibility to demonstrate compliance with the data security standards and programs operated by the card associations. Though Merchant Link's product delivers ongoing compliance with periodic updates and patches, other hardware or applications used by the merchant may not meet these stringent requirements, leaving the merchant vulnerable to breaches. **It is imperative that Merchants review the PCI DSS and PA-DSS standards, and complete the *PCI Self Assessment Questionnaire* to judge their own security practices.**

6.2 Merchants

Depending on annual transaction volume, PCI DSS requirements range from completing a self-assessment questionnaire to engaging an independent security assessor for conducting annual on-site security audits. Where merchants fit in this continuum is determined on annual transaction volume.

The Merchant (the end company receiving payment for goods and/or services) has ultimate responsibility for verification and compliance of PCI DSS. Contact your payment processor or review these requirements directly at
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
for more information. Through its partners and linkages to its NetVu service, Merchant Link can assist Merchants in becoming PCI compliant.

7 PA-DSS Requirements – POSLynx220 Specifics

The following sections correlate to the latest PA-DSS requirements, PCI PA-DSS Requirement and Security Assessment Procedures v1.2, describe the relevant items covered and how Merchant Link's POSLynx220 v2.12 meets these requirements through design or configuration. You will note in reading this section that most PA-DSS requirements have been met by designing conformance into the POSLynx220 product and thus do not require Partner/Merchant action or intervention in most cases.

The PA-DSS requirements that can be configured in the POSLynx220 are detailed in the specific sub-section tables with more complete instructions/actions provided in *the Partner Implementation and Configuration Notes* that follow each table. Other implementation guidelines are provided in the sections on access to the POSLynx220, later in this guide.

PA-DSS requirements that do not pertain to the POSLynx220 such as *PA-DSS Requirements, Section 6.0; Protect Wireless Transmissions*, have been included for completeness but primarily state that the general requirement is not applicable to the POSLynx220, as they are not directly supported. Should Partners wish to use Merchant Link products in solutions that would affect these requirements, Partners are responsible for securing all data and ensuring that all implementations meet applicable PCI requirements and that all equipment and applications used in the solution have been PA-DSS validated.

7.1 Storage of Cardholder Data (PA-DSS 1.x)

In order to simplify the tracking of Merchant Link's PA-DSS implementation, the remainder of this guide will detail how Merchant Link's POSLynx220 versions meet their PA-DSS requirements and any merchant configuration and/or partner notes associated with secure implementation as defined by the *Visa Payment Application Best Practices (*current reference document is *PA-DSS Requirements and Security Assessment Procedures, Version 1.2 October 2008).*
PA-DSS Requirement Specifics Partner/Merchant Action required

PA-DSS Requirement		Specifics	Partner/Merchant Action required
1.0	Do Not Store Magnetic Stripe, CVVS/CVC2 or PinBlock (PVV) Data in:	POSLynx220 does not store any sensitive cardholder data after authorization except, where instructed by processors, card number and expiry date needed for batch settlement.	None
1.1.1 1.1.2 1.1.3	- incoming transaction data - Transaction logs - all other logs - History files - Trace files - Non-volatile memory and cache - DB Schemas - DB contents	- no transaction data kept - transaction logs limited to first 35 chars with card numbers X'd out save for first six and last 4 numbers - No cardholder data stored in other logs - Diagnostic file sent to NetVu hold no cardholder data - N/A - No cardholder data stored - No sensitive data stored in DB - No sensitive data stored in DB	None None None None None None None None
1.1.4	Securely delete payment data stored by previous versions	New version downloads are disabled unless batches are closed (which clears stored payment data)	None
1.1.5	Securely delete crypto keys stored by previous versions	Keys generated at application level so pre-existing keys deleted with incoming version	None

Where applicable, the associated POS Application or device (ECR, POS terminal, POS Application interface, etc.) transmitting cardholder data is responsible for securely passing all sensitive authentication data (i.e. magstripe/CV/pin block) to TransNet application and estroying any sensitive data passed from the processor through to the POS application or payment device.

- The POSLynx220 v2.12 TransNet implementation connects to all important payment interfaces. In the POS Systems world, these use XML-based protocols that can be communicated to the TransNet payment engine using TCP/IP sockets or ActiveX controls and in the ECR space, they use either serial or TCP/IP sockets communication.

Partners should attempt to migrate POS applications that use a file drop mechanism to transfer payment transaction data to a more secure implementation. In situations where this is not possible the following points are critical:

- Both the POSLynx220 and the POS Application server should reside on the local side of the firewall.
- The Partner and Merchant should apply proper security by using permissions on any shared folder/directory and by limiting access to the shared folder/directory.
- When a file is written into the designated directory, the POSLynx220 will remove it within 50 ms when the POSLynx220 controls this process. It is the POS application's responsibility to destroy or encrypt the file that is written back. Certain POS Application implementations control the removal of all data from the shared drive themselves. Partners should review their documentation to verify correct procedures are used in these instances.

POSLynx220 v2.12 devices do not contain any sensitive data as logging functions are reviewed and tested upon each daily build/test cycle. That being said, nonproduction or customized software based on v2.12 are not tested against all working environments and could react oddly in un-verified environments. For this reason, these releases should generally be limited to test environments and field pilots.

- In situations where a debug version of v2.12 is needed for field use, the Partner and Merchant Link will work with the Merchant to ensure that no sensitive data is collected during the testing process.
- It has been Merchant Link's experience that typical field issues do not require inclusion of payment data to determine root causes.
- Certain protocols available on the POSLynx220's list of available Hosts do not have encryption capabilities and are meant to be used over private, secure networks. Partners should be careful to choose encrypted Hosts when connecting to public networks such as the Internet.
- V2.12 pre-auth transactions are defaulted to expire after 5 days (if not closed with post-auth or deleted by a close batch) with a maximum of 14 days for certain customers such as car rental companies. Partners should set this value to lowest level needed to match the merchants need (i.e. 1 day would be sufficient for a restaurant).

- Partners should be careful to close all batch settlements before attempting any upgrades as not doing so could result in failed downloads or potential balancing issues after the download.

- All cryptographic keys are generated at the application level and are created as needed by the application using multiple unique factors.

7.2 Protection of Stored Data (PA-DSS 2.x)

PA-DSS Requirement		Specifics	Partner/Merchant Action required
2.0	Protect Stored Cardholder Data	No cardholder data is stored after batch settlement	None
2.1	Guidance on cardholder data purging	No cardholder data is stored after batch settlement so no purging required	None
2.2	Mask displayed PAN	All card numbers are masked to last four digits	None
2.3	Render PAN unreadable, when stored	PAN stored and encrypted only when required for settlement, deleted afterwards	None
2.5	Protect encryption keys	Encryption keys are not stored but built as needed by application	None
2.6	Key management processes		None
	- Generation of strong keys - Secure key distribution - - Secure key storage - Periodic key changes - Destruction of old keys - Split knowledge of keys - - Unauthorized substitution - Revocation of keys - Key custodian acknowledgement	- Based on multiple factors within the POSLynx220 - Private keys are not distributed beyond the device - Keys not stored in device but generated on as needed basis - N/A - N/A - Keys not stored in device but generated on as needed basis - N/A - N/A - N/A	

7.2.1 Partner Implementation and Configuration Notes – PA-DSS 2.x

Merchant Link has attempted, wherever possible, to minimize security headaches for our customers and Partners by enforcing security requirements directly within the POSLynx220 device. The more limited the ability to alter security requirements, the more likely these requirements will not fall below the minimum.

- Cardholder data is not stored on device apart from requirement to store awaiting batch settlement. The stored data is not accessible to the customer (or anyone else) during this period so no data purging is required
- POSLynx220 with TransNet uses AES with a 256 bit key size so these settings are not configurable.

- Downloading new firmware to the POSLynx220 device will not over-write logs nor delete open batches although the POSLynx220 will prompt the user to close batches before download and will fail to overwrite firmware if a batch is still open.

Integrators should not need to add any steps, as neither audit logs nor syslogs hold any cardholder data. Any retained batches remain encrypted and PAN data un-accessible.

- Integrators should avoid downgrading POSLynx220 units from one version to a lower version (i.e. v2.12 to v2.10) as this may cause uncertain device behavior as the older version tries to rationalize the newer, extended configuration file.

One of the most important aspects of any cryptographic system is the creation, usage, maintenance and support of encryption keys within applications. When a POSLynx220 starts up, a series of events are triggered for secure cryptographic key support.
- Information is retrieved from the POSLynx220 device configuration for an encryption key location.
- This information is combined with fixed and random information to create a key source
- This source is then hashed using a MD5 cipher to generate the secure key
- Finally, the POSLynx220 attempts to decrypt a single known-value in the database, utilizing the expected good key in order to verify its accuracy prior to startup.

Implement key management processes and procedures: The POSLynx220's cryptographic policies happen at the application level and are not user configurable.

Both the encryption algorithm (cipher) used, as well as key length (strength) are pre-set by the POSLynx220 at build time as AES256 in all TransNet releases.

Note: *POSLynx devices running any release that do not create the payment packet to the processing host, but merely pass on a complete payment transaction from a fully functioning POS System, do not store any cardholder data. Some older versions, such as v2.08, do not support or maintain any encryption keys.*

7.3 Provide Secure Authentication Features (PA-DSS 3.x)

PA-DSS Requirement Specifics Partner/Merchant Action required
3.0 Use unique user IDs and secure authentication POSLynx220 allows unique, secure, multiple-user access to TransNet and payment GUI. No user access (admin or other) to cardholder data is allowed. None

PA-DSS Requirement		Specifics	Partner/Merchant Action required
3.0	Use unique user IDs and secure authentication	POSLynx220 allows unique, secure, multiple-user access to TransNet and payment GUI. No user access (admin or other) to cardholder data is allowed.	None
3.1	"Out of the box" unique user ID and secure authentication	All applications require unique user IDs and secure authentications for admin access. No user access to cardholder data is provided.	None
3.2	Access to servers and DBs with payment applications require unique user ID and secure authentication	Entire application resides on POSLynx220 device. This single access point uses unique user ID and secure authentication	None
3.3	Render application passwords unreadable	POSLynx220 does not store application passwords but instead stores a cryptographic hash of the original data merged with some random data. The application regenerates this random data as required to validate the password(s).	None

7.3.1 Partner Implementation and Configuration Notes – PA-DSS 3.x **Unique user IDs and secure authentication for admin users and/or access to cardholder data**

The POSLynx220 v2.12 running TransNet retains cardholder data until transactions are settled with the authorizing bank. This data is encrypted as per section entitled *Protection of Stored Data*. No access, from the POSLynx220 GUI or otherwise, is provided or allowed to retained cardholder data. The POSLynx220 v2.12 release forces users to change default passwords or passwords that have been reset from NetVu, to unique usernames and complex passwords upon first entry to device using these passwords.

User account set-up on the POSLynx220 v2.12 allows a wide selection of capabilities to be selected/deselected depending on the particular user requirement. Partners should establish user accounts that offer the minimum feature set required for the specific user. On devices running TransNet, admin access does not enable payment application permissions unless specifically allowed by the admin user. A separate user account should be established when payment applications need to be connected to TransNet or should payment transactions need to be run or administered directly from the POSLynx220 payment GUI.

One of the key benefits of using the POSLynx220 as a payment application is that the complete payment application resides on the POSLynx220 router/firewall; no other PC's, servers or databases need contain any cardholder data. As an additional security overlay, a feature key must be introduced into the POSLynx220 from NetVu to enable TransNet functionality.

Resetting the POSLynx220 to factory defaults removes all previous database, password, configuration and log files. When the device resumes contact to NetVu, it will receive its

feature key and then be able to use and have enabled features configured. Partners that do not see the required configuration options on the POSLynx220 GUI upon start-up, should verify their feature key is allowing the correct features (can be viewed in features.txt file in NetVu Diagnostics file under Advanced).

7.4 Log Payment Application Activity (PA-DSS 4.x)

PA-DSS Requirement Specifics Partner/Merchant Action required 4.0 Audit Logging activity
POSLynx220 tracks all required activity through its audit logs
None

PA-DSS Requirement		Specifics	Partner/Merchant Action required
4.0	Audit Logging activity	POSLynx220 tracks all required activity through its audit logs	None
4.1	Log all user access and activities "out of the box" and link to individual users (incl. admin)	Audit trail logging cannot be turned off within the POSLynx220, but can be deleted by users with appropriate permissions. This information is also sent to NetVu management server on scheduled basis.	None
4.2	Automated audit trail to track and monitor access	Audit logging cannot be turned off within the POSLynx220.	None

7.4.1 Partner Implementation and Configuration Notes – PA-DSS 4.x

POSLynx220 provides extensive logging of all access, system-level and payment transaction activities. Audit logging is not a configurable parameter and so the POSLynx220 will always be compliant with the associated PCI requirements.

The POSLynx220 is only responsible for audit trails of activities that interact with the POSLynx220. Other parties are responsible for logging activities outside of the POSLynx220 (i.e. POS application manufacturers have the responsibility to log connection attempts to the POSLynx220 – once connection request is received, either by dial, IP or another connection mechanism, it is logged from that connection level forward by the POSLynx220).

Logs can be deleted or access to logs set via account permissions established by the admin user through the POSLynx220 GUI. Partners can also change account permissions through Merchant Link's NetVu management server on POSLynx220's running v2.12. A history of POSLynx220 audit logs is sent to NetVu which stores this data for the required period.

7.5 Develop Secure Payment Applications (PA-DSS 5.x)

PA-DSS Requirement Specifics Partner/Merchant
Action required 5.0 Develop Secure Payment Applications POSLynx220 is a self-contained router running on proprietary hardware and so ships with no 3rd party applications and only the minimum application footprint. It is provided as a standalone payment router with TransNet payment engine (v2.12). Neither of these applications allow for third party developed extensions save for applications following Merchant Link XML spec. 5.1 Develop based on secure coding guidelines Merchant Link developers are trained in secure coding techniques and apply this training in developing our TransNet application. Security is not only included in our development cycle but in the solution concept itself, helping our customers and partners deliver simple, PCI-compliant solutions.

Generally no requirements for Partners. In certain cases Partners may need to test custom releases on unique equipment not available to Merchant Link.

PA-DSS Requirement		Specifics	Partner/Merchant Action required
5.0	Develop Secure Payment Applications	POSLynx220 is a self-contained router running on proprietary hardware and so ships with no 3rd party applications and only the minimum application footprint. It is provided as a standalone payment router with TransNet	None
		payment engine (v2.12). Neither of these applications allow for third party developed extensions save for applications following Precidia XML spec.	
5.1	Develop based on secure coding guidelines	Precidia developers are trained in secure coding techniques and apply this training in developing our TransNet application. Security is not only included in our development cycle but in the solution concept itself, helping our customers and partners deliver simple, PCI-compliant solutions.	None

		payment engine (v2.12). Neither of these applications allow for third party developed extensions save for applications following Precidia XML spec.	
5.1	Develop based on secure coding guidelines	Precidia developers are trained in secure coding techniques and apply this training in developing our TransNet application. Security is not only included in our development cycle but in the solution concept itself, helping our customers and partners deliver simple, PCI-compliant solutions.	None
5.1.1	- Changes/patches are tested prior to deployment	- Daily loadbuilds are tested via our automated regression testing system, "Sanity", validating most commonly used devices, protocols and features.	None
5.1.2	- Separate devel, test, and production environments	- Precidia has separate development, QA/certification and production environments	None
5.1.3	- Separation of development, test and production duties	- Precidia maintains separate personnel in these roles	None
5.1.4	- Live PANs not used for testing or development	- No live PANs are used in testing or development	None
5.1.5	- Remove test data and accounts prior to release	- All applications are built with only standard production accounts and no other test or custom data or accounts	None
5.1.6	- Remove custom accounts and data prior to release	- All applications are built with only standard production accounts and no other test or custom data or accounts	None
5.1.7	- Review of custom code prior to release to customers	- Custom code passes code review upon entry to Precidia's code repository and is tested within Sanity before shipment to customer - Precidia generally builds and tests its application code on a daily basis. Senior developers review new code submitted to Precidia's code repository for any changes that may affect security.	Generally no requirements for Partners. In certain cases Partners may need to test custom releases on unique equipment not available to Precidia.
5.2	Develop Secure Web Payment Applications	POSLynx220 v2.11 and v2.12 allow for eCommerce type web payment functionality in addition to GUI payment functions	None
5.2.1	- Cross-site scripting	- Verified	None
5.2.2	- Injection flaws	- N/A as no database	
5.2.3	- Malicious file execution	- Verified	
5.2.4	- Insecure direct object references	- N/A	
5.2.5	- Cross-site request forgery	- N/A, no auth credentials	
5.2.6	- Information leakage	- Verified	

5.2.7 5.2.8 5.2.9 5.2.10	- Broken authentication and session mgt - Insecure cryptographic storage - Insecure communications - Failure to restrict URL	- N/A, no session management - N/A - only SSL communications allowed - N/A, no session management	
5.4	No use of unsecured services/protocols	- No unsecure services are enabled by default for payment	Partners should require encryption across all unsecured networks

7.5.1 Partner Implementation and Configuration Notes – PA-DSS 5.x

Merchant Link's development approach integrates security at each stage of development. Because Merchant Link exclusively develops applications (and any application changes to the POSLynx220), Partners can be assured that integrated security remains a key component from development to production through to deployment and configuration in the field.

POSLynx220 is a self-contained environment and is designed to offer maximum security by placing TransNet behind its onboard routing firewall. This firewall ships with all incoming ports blocked from outside access. These firewall settings should remain in the default configuration to maintain the merchant's PCI security. If any ports are opened, Partners should be careful to ensure this access conforms to the relevant PCI requirement(s) if any.

TransNet v2.12 hides access to HTTPS (port 443) and SSH by default. Partners wishing to access the POSLynx should configure Port Forwarding rules to allow access from a specific IP Address or range and route this path through to the applicable port on the POSLynx220's

LAN port. More information on this configuration is available by contacting Tech Support at Merchant Link or by accessing this documentation on our Partner wiki.

Partners should ensure that they or their merchants implement policies to remain PCI compliant (please see section on *Administrative Access to POSLynx220*). In cases where Partners perform incremental testing in their own or their customer's labs, care needs to be taken to remove all default passwords, logs and other data and configuration details that should not be moved to a live site. In order to do this consistently, Partners should return test units to factory defaults (refer to *Product User Guide* for process) or use only new units in customer sites.

7.6 Protect Wireless Transmissions (PA-DSS 6.x)

Merchant Link's products are not generally implemented within wireless networks, particularly 802.11 type implementations. In certain cases, wireless cellular networks can be used as a WAN back-up facility.

7.6.1 Partner Implementation and Configuration Notes – PA-DSS 6.x

- Partners should work with their wireless carrier providers to ensure adequate security (such as data VPN's) is provided for payment applications.
- Merchant or Partner Network Administrators should provide security policy and settings for any wireless implementations.
- Partners should use encryption, like SSL, whenever using the POSLynx220 over a wireless network.

7.7 Test for Payment Application Vulnerabilities (PA-DSS 7.x)

Merchant Link's POSLynx220 devices are validated for compliance with following development processes:
PA-DSS Requirement Specifics Partner/Merchant
Action required

PA-DSS Requirement		Specifics	Partner/Merchant Action required
7.1	Process to identify newly discovered security vulnerabilities	- Precidia monitors and uses information from outside security sources for vulnerability assessment and policy - POSLynx220 is tested against new 'identified' vulnerabilities, when and where applicable	Ensure any potential security issues are directly communicated to Precidia Support. - maintain NetVu support on all POSLynx220's
7.2	Process for timely development and deployment of security patches and upgrades	- patches/upgrades deployed as soon as securely possible - NetVu utilized as a secure conduit for timely deployment of any patches/updates within a known chain of trust. - deployed patches are verified prior to installation	- work with end clients to aid in timely migration - Generally no requirements for Partners. In certain cases, Partners may need to test updates on unique equipment not available to Precidia. - all patches are verified by our automated Sanity test station

7.7.1 Partner Implementation and Configuration Notes – PA-DSS 7.x

Although Partners are responsible for testing associated network applications for vulnerabilities outside of the POSLynx220, the POSLynx220 code is written and tested exclusively by Merchant Link, which limits the work and efforts needed from our Partners. Partners' access to NetVu provides the tools needed to track customer application version levels and conformance to any customer or Partner network procedures that may be in place. NetVu also maintains the integrity of the update as filenames are changed each time a firmware download is requested and the location is sent within the command to the end device.

Merchant Link will work with Partners to create tailored communications plans that help ensure customers understand the need to continually remain on the latest certified version. Using information from NetVu, communication on particular security issues will be targeted only to Partners or Partners' customers that are directly affected by the specific issue.

7.8 Facilitate Secure Network Implementation (PA-DSS 8.x)

PA-DSS Requirement		Specifics	Partner/Merchant Action required
8.1	Payment application must be implemented into a secure environment	All POSLynx220 releases interoperate seamlessly in all network implementations and will not	Only change default settings when clear need
		interfere with required services unless specifically programmed to do so	and when this does not reduce overall system security

7.9 Cardholder Data Not Stored on Internet Connected Server (PA-DSS **9.x)**

PA-DSS Requirement		Specifics	Partner/Merchant Action required
9.1	Application must not require the web server and the database server be on the same server	POSLynx220 with TransNet has no programmatic access between web server and database. It uses a proprietary database with no external visibility.	None

7.9.1 Partner Implementation and Configuration Notes – PA-DSS 9.x

The POSLynx220's on board router acts as the DMZ for our TransNet payment application. This PABP requirement was written to preclude unauthorized parties gaining access to the database simply by breaking into the application's web server.

Even if unauthorized parties were to gain access to the POSLynx220's web server, there is no programmable connection between the web server and the database and so no access to the database could be gained.

7.10 Facilitate Secure Remote Software Updates (PA-DSS 10.x)

PA-DSS Requirement		Specifics	Partner/Merchant Action required
10.1	Secure remote software updates	Upon a request by an authorized NetVu user, software updates and upgrades are loaded onto NetVu download server for a limited period. NetVu cannot contact any device, so when device next contacts, hashed filename and download location are sent to the field device	None. Partners should always use Precidia's NetVu server to manage field devices

7.10.1 Partner Implementation and Configuration Notes – PA-DSSP 10.x

Merchant Link's NetVu server supports firmware updates (as well as other features such as configuration downloads) using a "subscribe/pull" method, so no outside-in remote access to installed devices is required. The Partner need only log into the NetVu server managing their devices and enters the commands they wish to deliver to the particular enrolled device (firmware download, configuration download, etc.). The server stores these until the next device contact. If required, contact can be "forced" by the customer or Partner by pressing the device's recessed "Action" button or simply by power-cycling the device.

Devices must be enrolled by a unique serial # into the NetVu server before NetVu will respond to the device. This serial #, actually the device's MAC ID, is then used as a password, allowing NetVu to differentiate between products and providing an extra level of security.

Merchant Link will generally inform the purchaser of POSLynx220 support via email that a particular product(s) needs to be upgraded to the latest version. It is the Partner's responsibility to inform and work with the end customer to determine whether, how and when particular upgrades should be implemented in their customer's environment(s).

7.11 Facilitate Secure Remote Access to Payment Application (PA-DSS 11.x)

PA-DSS Requirement		Specifics	Partner/Merchant Action required
11.1	- Application must not interfere with two factor authentication	- Precidia's POSLynx220 applications do not interfere with any two factor authentication implementation	None
11.2	- Remote access must use two factor authentication mechanism	- POSLynx220 uses username/password and SSL (or SSH) for authentication	None
11.3	- Remote access must be implemented securely	- NetVu should be used whenever remote access to a POSLynx220 is required - POSLynx220 enforces the following security when accessing the GUI: - all communication is encrypted using HTTPS -device access to NetVu filtered by registered Serial # (MAC address) - Partners are never logged onto end device via NetVu - passwords conform to PCI standards - access to device and NetVu is logged	None, although Partner should follow implementation notes below

7.11.1 Partner Implementation and Configuration Notes – PA-DSS 11.x

As stated earlier in this guide, Partners should use NetVu to communicate with the POSLynx220 whenever possible, both for issuing commands for the POSLynx220 and for reviewing device logs, configuration files, etc. In the few situations where direct access to the POSLynx220 GUI might be required, all POSLynx220 releases enforce the use of SSL to

access the GUI via the WAN interface. POSLynx220 v2.12 allows enhanced diagnostic access to the POSLynx220 via SSH to a non-standard port. The requirement for unique userids and complex passwords also applies to this access method.

Default router settings block all outside (WAN) access save for HTTPS (to port 443) for POSLynx220 configuration GUI access. Partners should verify that all unblocked services/ports are kept to an absolute minimum. Services required on an occasional basis can and should be configured on an as-needed basis (ideally through NetVu) and removed as soon as no longer required.

Merchant Link has specifically developed its NetVu management server to manage remote devices without having to establish connections into those devices and instead, having the device connect to NetVu. Connecting into NetVu allows Partners to access a limited set of commands without opening up the entire device to control by an outside user.

Although we highly recommend that Partners use NetVu for remote admin, should other remote access methods or applications be used to access systems, Partners should be sure to follow the guidelines set out below:
- change default passwords in remote access software
- use strong authentication/complex passwords for logins
- filter incoming connections on known IP Addresses/MAC IDs, particularly useful for external HTTPS and SSH access from known IP Addresses
- enable encryption on data transmissions
- lockout user after certain number of failed login attempts
- establish connections through a VPN
- ensure logging is enabled
- restrict access to customer passwords on a need to know basis
- set customer passwords according to PCI DSS 8.1, 8.2, 8.4, and 8.5

Configuration Note: Partners should be particularly careful when changing the state of the WAN interface to Manual Static from DHCP or vice versa, ensuring that IP Addressing is correct for the site. Saving an incorrect address scheme from a NetVu template could effectively disable the WAN access both for NetVu and remote access, requiring an on-site technician to access the device locally or a reset to factory defaults.

7.12 Encrypt Sensitive Traffic Over Public Networks (PA-DSS 12.x)

PA-DSS Requirement		Specifics	Partner/Merchant Action required
12.1	- Use strong cryptography to safeguard cardholder data over public networks	- POSLynx220 never sends cardholder data to NetVu or any other location but processor - POSLynx220 uses SSL when communicating to SSL processing hosts	Use SSL over public networks (SSL2.0, TLS1.0 with medium and high encryption algorithms)
12.2	- do not send unencrypted PANs by email	- Precidia and/or the POSLynx do not send PAN data via email	None.

7.12.1 Partner Implementation and Configuration Notes – PA-DSS 12.x **Partners should never send unencrypted payment transaction or other sensitive data over public networks**

Merchant Link builds SSL connectivity into all protocols going over public networks such as the Internet. Partners should ensure that any processor Hosts configured in a POSLynx220 connected to a public network, have the ability to receive SSL (and certificates). The POSLynx220 will enforce SSL use for known SSL hosts but Partners are still responsible for configuring the POSLynx220 to connect to SSL Hosts when going over public networks or routing unsecured transactions over secure networks (private networks, VPN's, etc.).

7.13 Encrypt All Non-Console Administrative Access (PA-DSS 13.x)

PA-DSS Requirement		Specifics	Partner/Merchant Action required
13.1	Encrypt all non-console administrative access	Access to configuration GUI is only allowed via HTTPS as described in 6.11 above. On v2.12 releases, SSH access on a non-standard port is allowed (not configurable).	None. Contact Precidia Support should emergency access be required

7.14 Maintain Instructional Doc'n and Training Programs (PA-DSS 14.x)

PA-DSS Requirement		Specifics	Partner/Merchant Action required
14.2	- Develop & implement training and communication plans	- Precidia has launched a Partner Resource Wiki allowing Partners to view training videos, FAQ's, PABP/PA-DSS Implementation Guides and other necessary documentation	Use the doc'n & training tools made available by Precidia on its Wiki and elsewhere.

7.14.1 Partner Implementation and Configuration Notes – PA-DSS 14.x

Merchant Link has recently launched our Merchant Link's Partner Resource Wiki, which offers a large selection of helpful documentation and training for our partners. The Wiki is focused on implementation and support issues commonly faced by our POS Partners, including security concerns. PA-DSS and PABP questions including latest validations, certified processors, PA-DSS Implementation Guides and other relevant documentation has been grouped together in the PA-DSS section of the Wiki.

Content is being added to our Wiki on an ongoing basis so Partners should log onto and review all materiel, including relevant PABP/PA-DSS content, on a regular basis.

Typical implementations layouts, including all relevant cables along with detailed, specific configuration instructions and screen shots are also proving to be very useful for our partners.

Note: The Wiki allows for partners to be notified when certain sections or pages are changed. Should partners be interested in setting up this function to stay on top of PA-DSS related changes, they can just enter a comment on the Wiki or send a request to support@Merchant Link.com or sales@Merchant Link.com.

8 TransNet on POSLynx - Implementation Considerations

8.1 Administrative Access

In certain situations, Partners may need to add an admin account to the existing 'Merchant Link' admin user account. In most instances, Partners should not need to add more users and should actively dissuade customers from adding more accounts that have access to the POSLynx220 unless required for direct application connectivity.

- All users can be administered by 'Merchant Link' user.
- POSLynx220's running v2.11 or v2.12 allow other admin users to be created and given permission to administer all users. Partners should limit the number of admin users set on a POSLynx and should instead allow only the functions required by the particular user.
- Partners and their customers can and should use Merchant Link's NetVu deployment and management server's Reset Password ability when working through lost passwords issues on prior versions. Partners using v2.10 and greater can change user passwords on NetVu by accessing a POSLynx220 Diagnostic file, clicking on the *uid_pwd.file*, changing the relevant password(s) and saving this to the device.

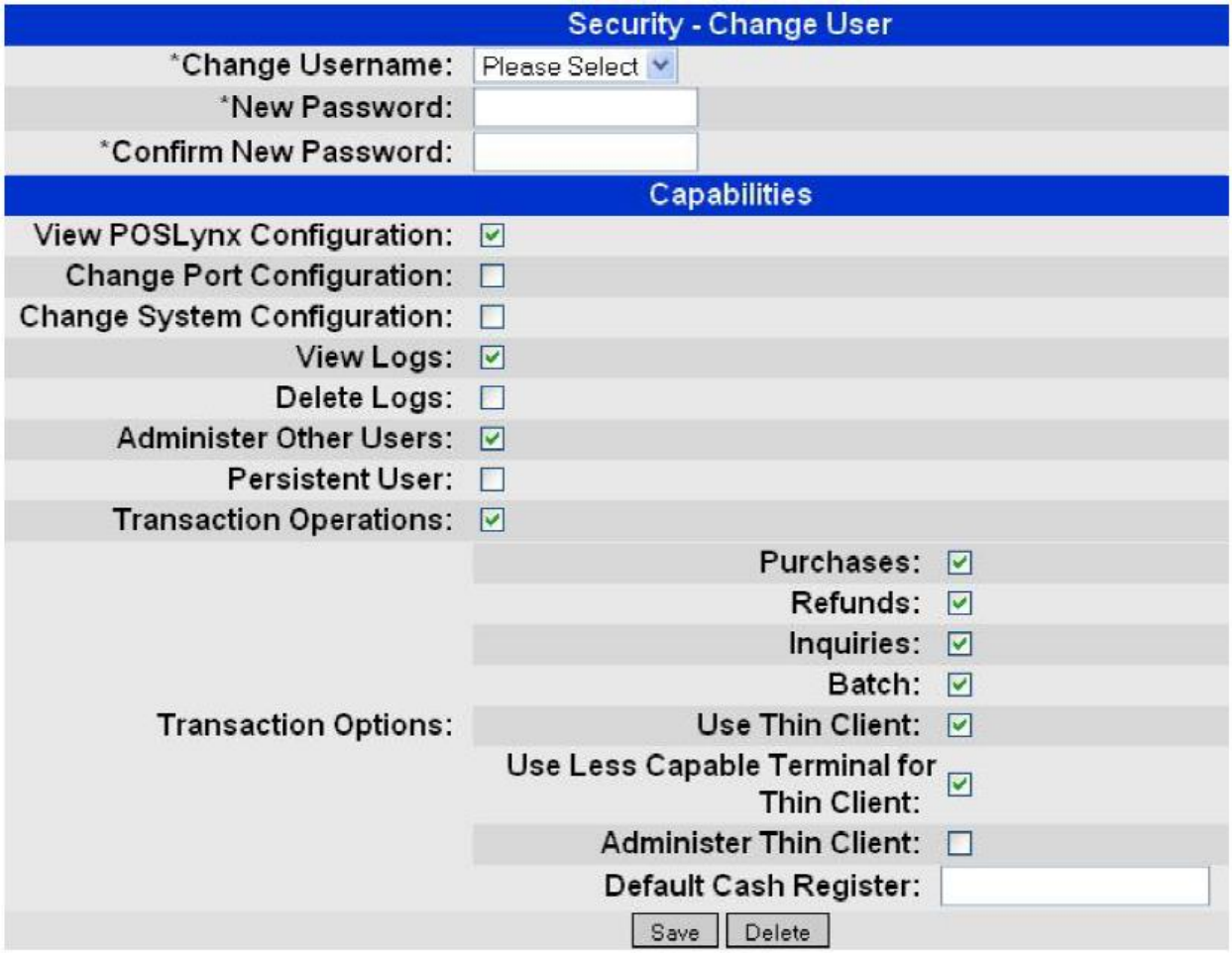
This capability allows Partners to remotely change passwords to the default 'Merchant Link' admin user even though the POSLynx220 forces users to change their NetVu issued passwords upon first entry to the device, thereby reducing the risk intercepted passwords pose, Partners should always use secure communications methods when communicating newly issued passwords to their customers

Partners should be aware that NetVu can only change passwords to 'Merchant Link' default user on v2.08 and v2.09 releases whereas NetVu can change all user passwords on the POSLynx220 v2.11 and v2.12.

Should Partners wish to remove NetVu Reset Password capabilities, they should delete Merchant Link user from Security => Tools menu

Removing the 'Merchant Link' user effectively locks-in existing users unless another admin user has been added prior to deleting the 'Merchant Link' user. The only way to add/alter user(s) at that point would be to reset device to factory defaults, resetting all users.

Partners wanting to disallow the ability to delete 'Merchant Link' users can check the Persistent User checkbox on v2.12's Security page (displayed below)



8.2 Administrative User Permissions

The POSLynx220 administrative account on v2.12 has master privileges for administering any and all user accounts within the system. The POSLynx220 enforces PCI password requirements including:

- Passwords should be at least seven (7) characters long including at least one number and one lowercase and one uppercase alphabetic character
- Passwords should be changed every 90 days
- Passwords should not be repeated/re-used in up to 4 changes
- Users should be restricted from further login attempts after failing six (6) consecutive attempts

8.3 Typical User Set-up

Specific differences exist in how administrative privileges are dealt with in v2.08 and newer releases, with a narrower range of user set-up options available in v2.08. A standard installation process by version might look like the following:

POSLynx220 running TransNet v2.12
Upon receiving a new POSLynx220 device, the system administrator will log into the POSLynx220 web GUI using userID=precidia and password=abc
The POSLynx220 will display a webpage requesting the admin user change the default password to a PCI compliant password.
The POSLynx220 will kick the user back to the login screen to log into the device with the newly created password.

Admin user can now add other users to the POSLynx220 configuration – for example, we could add a user called '*TestUser*'
Admin user sets *TestUser* password (enforced to PCI standards) and access permissions as per screen shot above
POSLynx220 allows multiple, simultaneous user access using different user IDs
Upon *TestUser* login, only permissions set by admin user are displayed or allowed (on Menu bar as well as on specific GUI pages)
The admin user can now set up roles for running payment transactions through device accounts with varying permissions for other users or incoming payment applications requiring secured access.

9 Reference Links

9.1 Card Association Links

Visa: http://usa.visa.com/merchants/risk_management/cisp.html
Master Card: http://www.mastercard.com/us/merchant/security/index.html
American Express:
https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US

9.2 Related Technologies

Linux: http://www.kernel.org/
http://www.uclinux.org/
SSL: http://www.openssl.org/

9.3 References

This document heavily references the PCI Council and, to a lesser extent, the Visa PABP and CISP websites located at www.pcicouncil.org and www.visa.com/cisp/. In many instances, configuration notes and suggestions are derived from the most current Merchant Link product User Guides located at www.MerchantLink.com or the Merchant Link Partner Resource Wiki (access is restricted but applications are available from our website by clicking on our Partner link at www.MercantLink.com).