ExaDigm Integrator 1.00.xx PA DSS Implementation Guide

NO WARRANTY

No warranty although ExaDigm has attempted to ensure the accuracy of the contents of this manual. This manual may contain errors or omissions. This manual is supplied "as-is," without warranty of any kind, either expressed or implied, including the implied warranties of merchantability and fitness for a particular purpose.

LIMITED LIABILITY

Limited Liability in no event shall ExaDigm be liable for any indirect, special, incidental, or consequential damages including damages for loss of business, profits, or the like, even if ExaDigm or its representatives have been advised of the possibility of such damages.

1.0 Revision History

Note: This PCI PA-DSS Implementation Guide (further referred to as IG) must be reviewed on annual basis, whenever the underlying application changes or whenever the PA-DSS requirements change. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users. ExaDigm will distribute the IG to new customers via a downloadable document on a customer serviceportal.

Date	Version	Author	Revision Description
12/11/2016	1.00	Rosalie Krondak	Initial
01/15/2017	1.01	Alex Grigoryev	Updated with PA-DSS requirements
01/21/2017	1.02	Alex Grigoryev	Additional procedures edited
01/25/2017	1.03	Rosalie Krondak	Formatting
02/03/2017	1.04	Rosalie Krondak	Added Final version numbers
03/25/2017	1.05	Rosalie Krondak	Updated per PA QSA feedback
04/02/2017	2.0	Bryan Schmidt	Final Release
06/09/2017	3.0	Chuck Maggs	Version for N5

2.0 Table of Contents

This page intentionally left blank.

3.0 Important Notice

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

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

The end user may undertake activities that may affect compliance. For this reason, ExaDigm is required to be specific to only the standard software provided by it.

4.0 Introduction

This document describes the steps that must be followed in order for the ExaDigm Payment application installations to comply with Payment Application – Data Security Standards (PA-DSS). The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (version 3.2 dated May, 2016).
The Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS) is comprised of fourteen requirements that support the Payment Card Industry Data Security Standard (PCI DSS). The PCI Security Standards Council (PCI SSC), which was founded by the major card brands in June 2005, set these requirements in order to protect cardholder payment information. The standards set by the council are enforced by the payment card companies who established the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.

5.0 PA-DSS Requirements for Compliance

5.1 Implementation Guide Purpose

This document is provided as an Implementation Guide to instruct the end user and resellers/integratorson secure product implementation and to document the secure configuration specifics mentionedthroughout the PCI PA-DSS requirements documentation. The document delineates vendor,reseller/integrator, and customer responsibilities for meeting all compliance requirements. It provides thedetails for how the customer and/or reseller/integrator should enable security settings within thecustomer's network. As an example, the Implementation Guide covers responsibilities and basic featuresof password security even though this is not controlled by the payment application, so that the customerand/or reseller/integrator clearly understand how to implement secure passwords for compliance.It is highly recommended that the vendor, reseller/integrator, and customer level users familiarizethemselves and adheres to PCI DSS standards available at:

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Special notes:

- Failure to adhere to PCI security compliance requirements may result in revenue loss and legalconsequences.
- Adding, altering and/or changing IP protocols, Services, Security Protocols supplied by ExaDigminvalidates the PA-DSS approval granted on tested set of tools and libraries. Software applicationprocessing of financial transactions must use TLS v.1.2, or HTTPS libraries and tools provided byExaDigm in order to secure the data in compliant fashion.
- All vendor, reseller/integrator, and customer level users are encouraged to register for securityupdates via an email sent to compliance@exadigm.com .

- If a vendor, reseller/integrator, and customer level users become aware of an existingvulnerability, they should inform ExaDigm by sending an e-mail to compliance@exadigm.com.

5.2 Implementation Guide Target Audience and Distribution

This document is intended for the end users, resellers and integrators who place ExaDigm products in service for processing credit card and debit card transactions, the ExaDigm product is deployed with ExaDigm Payment Applications or custom developed payment applications adhering to PCI PA-DSS requirements referred above.
The typical users, resellers and integrators include but are not limited to:

- ISO (Independent Sales Organizations)
- POS equipment distributors
- Payment Software Application developers
- Payment Systems Integrators
- Payment Processors
- Banks
- Merchants of all categories and payment industries accepting credit and debit cards

All categories of ExaDigm customers are encouraged to read the Implementation Guide at the event of purchasing an ExaDigm product. The document is available on the ExaDigm Inc. website: www.exadigm.com.
As an alternative option the document can be delivered by e-mail, fax or postal service to customers who choose to receive a hard copy. The Customer Account Manager is responsible to deliver the Implementation Guide and new revisions of the Implementation Guide to each customer as requested.

5.3 Implementation Guide Maintenance Policy

This Implementation Guide is subject to annual review and maintenance updates, which address the changes implied by new revisions of the PCI DSS and PCI PA-DSS standards as well as any software updates related to improvement of the security features in ExaDigm products.
ExaDigm Security Officer is responsible to maintain the Implementation Guide and perform annual review with ExaDigm PCI Compliance Committee. ExaDigm PCI Compliance Committee is required to review and approve the updated version of the Implementation Guide. The Customer Account Manager is responsible to notify customers of the updated copy as defined in the paragraph “1.2 Implementation Guide Target Audience and Distribution”.

6.0 PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PCI PA-DSS, PCI DSS, etc.):

- Payment Applications Data Security Standard (PCI PA-DSS) https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml
- Payment Card Industry Data Security Standard (PCI DSS) https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- Open Web Application Security Project (OWASP) http://www.owasp.org
- SEI CERT Coding Standards, https://www.securecoding.cert.org/

7.0 PCI PA-DSS vs. PCI DSS

ExaDigm's responsibility as a software vendor of a payment application is to ensure continuous compliance of its application to PCI PA-DSS standard.

ExaDigm's compliance team has performed an assessment and compliance review with the Qualified Security Assessor, an independent security assessment firm, to ensure that our software platform does conform to industry best practices when handling payment related information.

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

On the other hand, PCI DSS Compliance is a responsibility of a merchant and merchant's service providers, and is an assessment of merchant's actual payment acceptance environment.

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

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the PCI DSS apply to all members, merchants, and service providers that 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 included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

8.0 Application Overview

The ExaDigm Integrator version 1.00.xx Payment Applicationis a robust Point of Sale (POS) terminal application enabling secure payment acceptance on the ShenZhen Xinguodu Technology Co. Ltd PCI PTS POI device: N5.

The functionality of the ExaDigm Integrator application is accessed via a caller application; the caller application can be provided by ExaDigm, or the caller application may be created by a third party developer. In either case, the caller application can only perform the operations which the Integrator application permits and supports.
Only one ExaDigm Integrator application may be installed per device for payment card related operations. A merchant may have more than one payment terminal device deployed on a local network. A merchant may operate the N5 device in a broadband public Internet environment.
The ExaDigm Integrator application implements non-card data entry, such as transaction type, amount, address verification data elements, and other payment industry specific application functionality. It collects cardholder data strictly within PCI PTS certified POI environment and implements the complete payment processing functionality according to integrated Payment Processing Host specifications.
The ExaDigm Integrator operates in Card-Present and Card-Not-Present modes.
Supported card entry modes:

- Magnetic Stripe
- Contact EMV
- Contactless EMV (NFC)
- Manual Card Data Entry (PAN, Expiration Date and V-code (CVV, CVC, CID)

All card data entry operations are performed strictly on a PCI PTS 3 4.x certified PED POI. Supported POI device:

- N5, PCI 4.x Approved

Card is swiped or otherwise presented on a POI and is not exposed outside of the POI PCI PTS. No clear-text data is exposed or otherwise passed back.
The ExaDigm Integrator application never stores cardholder data.
Beyond the hardened Android 5.1.1 (Lollipop) operating system used by the supported N5 Terminal, there are no additional 3rd party software components.
ExaDigm Integrator is a standalone payment application designed for deployment strictly on the N5 hardware family of PCI PTS certified hardware terminals.
A typical deployment environment:

- A tier 3 or 4 Merchant
- One or more N5 terminal devices per location
- Local Area Network or broadband internet, or registered wireless module in N5

The ExaDigm Integrator application is sold or otherwise licensed by ExaDigm as a bundle, together with a caller application the N5 POS terminal. The end user acquires a license to run and operate the ExaDigm Integrator for payment card acceptance purposes.
The ExaDigm Integrator is designed for the following industries where credit/debit/EBT card payment acceptance is required:

- Retail Stores
- Restaurants, Bars
- Mail Order/Telephone Order (Card-Not-Present)
- Hotel/Lodging

9.0 Implementation Guide

The ExaDigm Integrator is always installed with the PCI PA-DSS configuration enforced. There are no configuration options available to the end user, which can affect

security configuration of the app.ExaDigm suggests that a test credit card transaction should be performed following any card acceptance parameter configuration update and/or app version upgrades.

9.1 PA-DSS Requirement 1.1.4

Securely delete any magnetic stripe data, card validation values or codes, and PINs or PIN block data stored by previous versions of the payment application, in accordance with industry-accepted standards for secure deletion, as defined, for example by the list of approved products maintained by the National Security Agency, or by other State or National standards or regulations.

9.1.1 Software Vendor Control Responsibility

- This is the initial release of the ExaDigm Integrator software for the N5 Terminal. No previous versions exist beyond test versions. Installation of the ExaDigm Integrator software for the N5 Terminal occurs prior to your receipt. Any update to the ExaDigm Integrator software will result in the complete erasure of any previous information stored by the previous version of the ExaDigm Integrator software.

9.2 PA-DSS Requirement 1.1.5

Securely delete any Sensitive Authentication Data (SAD, or pre-authorization data) used for debugging or troubleshooting purposes from log files, debugging files, and other data sources received from customers, to ensure that magnetic stripe data, card validation codes or values, and PINs or PIN block data are not stored on software vendor systems. These data sources must be collected in limited amounts and only when necessary to resolve a problem, encrypted while stored, and deleted immediately after use.

9.2.1 Software Vendor Control Responsibility

- ExaDigm will not collect or request SAD as part of our troubleshooting processes.

9.2.2 Customer Responsibility

If you as the merchant elect to capture sensitive authentication data for troubleshooting purposes, you must adhere to the guidelines below:

- Sensitive authentication data (pre-authorization) must only be collected when needed to solve a specific problem.
- Such data must be stored only in specific, known locations with limited access.
- Only collect a limited amount of such data as needed to solve a specific problem.
- Sensitive authentication data must be encrypted while stored.
- Such data must be securely deleted immediately after use.
- Note that there is no method within the ExaDigm Integrator or N5 Terminal to collect this information. You must use some third-party means for this collection. Such collection will not be supported by ExaDigm troubleshooting personnel.

9.3 PA-DSS Requirement 2.1, 2.2 &2.3

Cardholder data must be deleted after it exceeds the customer defined retention period. All locations where payment application stores cardholder data must be deleted. Full PAN is never printed or displayed by the application.PAN must be encrypted via strong cryptography with associated key management processes and procedures

9.3.1 Software Vendor Control Responsibility

Cardholder data, whether encrypted or not, is never stored on the device. Only the last four digits shall be displayed on the terminal or printed in the receipt. The remaining cardholder number is masked with asterisk (*). Cardholder data is only displayed on the terminal screen and on the receipt.
Truncated PAN display is enabled by default and may not be changed.Truncated PAN is also displayed in the following areas:

- Terminal Receipt
- Terminal Entry Screen

The N5 terminal and ExaDigm Integrator are pre-configured upon shipping to prevent in inadvertent capture of cardholder data. This cannot be modified and does not require any configuration changes by the merchant. Tampering with the PTS POI device itself is not permitted and will violate your PCI DSS status.
The ExaDigm Integrator software is pre-configured to encrypt cardholder data following a DUKPT key management scheme using a pre-injected key with a 192-Bit 3DES algorithm. This key and key management scheme allows for a unique key per transaction and does not require any configuration changes by the user.

9.3.2 Customer Control Responsibility

In order to qualify for the best processing rates, settlement should occur every day. If using manual settlement, be sure that transaction settlement of the device is part of the end of day procedures. Be sure to review the settlement report that prints when the batch settlement is complete to ensure that a “Settlement Successful” message is printed.
The ExaDigm Integrator software on the N5 Terminal does not store any cardholder data. If for some reason you store the PAN for debugging purposes outside of the ExaDigm Integrator application, you must protect this data per PCI DSS guidelines, stop collecting once troubleshooting is completed, and secure deleted this data once troubleshooting is completed.

9.4 PA-DSS Requirements 2.4, 2.5, 2.5.1-2.5.7, & 2.6

Software vendor must provide guidance to customers to protect keys used to secure cardholder data and secure key management.Vendor must provide a mechanism to render irretrievable cryptographic key material or cryptograms stored by the payment application.

9.4.1 Software Vendor Control Responsibility

There are no specific settings required for the ExaDigm Integrator application to delete cryptographic key material from the N5 device.
The ExaDigm Integrator application does not store any sensitive authentication data at any time. There is no method for re-encrypting historical data with new keys since no such data exists.

9.4.2 Customer Control Responsibility

You must ensure that the batch is settled daily. Customers do not have access to injected keys. There is no interaction required by you for key management. If you believe your PINPAD has been tampered with, you should have the N5 terminal returned to ExaDigm support and a new terminal will be provided to you.
The only method in place to change the initial key injected into the device is to return the device for re-keying and injection. If you return the N5 terminal,a new ExaDigm terminal will be issued. This process of re-keying and injection will ensure that the previous initial key is securely wiped and that new unique keys are created.

9.5 PA-DSS Requirement 3.1, 3.2, & 3.3

Software vendor must enforce use of unique user IDs and secure authentication for administrative access and access to cardholder data.

9.5.1 Software Vendor Control Responsibility

N5 devices use a stripped-down version of the Android Operating System that has tightly controlled interactive user capabilities. The ExaDigm Integrator application components are always running under a standard unprivileged system user account and don't have access to system critical areas of the underlying Operating System. A running ExaDigm Integrator application has full access to its home directory only.
The following security policies are enforced:

- No user has access to cryptographic material, security sensitive data and authentication data.
- The ExaDigm Integrator has a secure authentication system that provides access and enables them to process operations through the application based on a unique set of credentials. A complex password policy is enforced for all roles.
- Above password requirements are needed for any device on the same network as your N5 terminal or within your card environment.

9.5.2 Customer Control Responsibility

It is the responsibility of the Customer to ensure that all users establish and maintain unique user IDs and secure authentication password per the policy specified in this PA-DSS Implementation Guide and according to PA-DSS Requirements 3.1.1 through 3.1.11. This means you must setup accounts for each user and not allow for group or shared accounts. Password settings are enforced by default and do not require any changes from the end-user.

9.6 PA-DSS Requirement 4.1 &4.4

Software vendor must implement and enforce automated audit trails and support the ability for centralized logging.

9.6.1 Software Vendor Control Responsibility

The Exadigm Integrator when called requires an APIKEY, a Token, a User id and a Password assigned to the merchant. This input combination allows for the Caller to be validated at three levels (Security, Software & Processors).

ExaDigm Integrator implements automated logging as follows:

- This logging is required for your PCI DSS compliance and this why they cannot be disabled;
- Events logged with date/time stamp, Terminal Id and user ID:
    - Audit log initialization
    - User access event (logon, logout), successful and unsuccessful
    - Number of unsuccessful access attempts
    - Lockout events
- Terminal can also be automatically Locked Out. When more than two users fail logging

9.7 PA-DSS Requirement 6.1, 6.2, &6.3

Software vendor must provide guidance to customers regarding secure configuration of wireless network access parameters as well as guidance for wireless network setup and configuration.

9.7.1 Software Vendor Control Responsibility

ExaDigm Integrator does not use vendor default encryption keys, passwords,or SNMP community strings. The ExaDigm Integrator relies on the Customer to implement a secure wireless network environment or configuration.

The ExaDigm Integratormay use wireless communication to communicate with the external systems/services as defined in paragraph "Appendix C" as it is bundled with a defined PCI PTS ShenZhen PTS POI terminal N5. This classifies ExaDigm Integrator as a category 1 wireless payment application.

The ExaDigm Integratoruses industry best practices (IEEE 802.11.n) to ensure the strong encryption for network access authentication and data transmission.

9.7.2 Customer Control Responsibility

It is the responsibility of a Customer to ensure that following actions are taken to implement secure wireless communication environment when Wi-Fi communication technology is used in Merchant environment:

- It is required to change all default encryption keys, passwords and SNMP community strings (if applicable) on all network equipment at the time of installation for all wireless components accessible by the ExaDigm Integrator.

- A customer must implement procedures for changing wireless encryption keys and passwords, including SNMP strings, anytime anyone with knowledge of the keys/passwords leaves the company or changes positions.

- Written instructions must exist for changing default encryption keys, passwords, and SNMP community strings on any wireless components installed at Merchant location and accessible/used by the payment application.

- A firewall between any wireless networks and systems that store cardholder data must be installed and configured securely in compliance to PCI DSS requirements. A firewall must be configured to deny or — if such traffic is necessary for business purposes — permit only authorized traffic between the wireless environment and the cardholder data environment.

- firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks. All N5 Terminals are shipped with the latest firmware.

- other security-related wireless vendor defaults must be changed, if applicable.

- wireless networks transmitting cardholder data or connected to the cardholder environment must use industry best practices to implement strong encryption for authentication and transmission.

The wireless environment must support WPA2 with PSK or AES authentication and security. This is the only option supported within the ExaDigm Integratorapplication. During the setup of the N5 Terminal device, you will be requested to connect to your WiFi network and supply needed information for connectivity. This will happen as soon as you turn the device on. Until connectivity to a deployed WiFi network is performed the device will not move past the setup phase.
The ExaDigm Integrator uses your wireless network to communicate with you merchant acquirer, and this is done over a TLS 1.2 connection so as to not rely on your wireless network's security to secure data transmission.

9.8 PA-DSS Requirement 7.2.3

Software vendor must provide instructions to customers regarding secure installation of patches and updates.

9.8.1 Software Vendor Control Responsibility

It is a Software Vendor responsibility to:

- Make the most recent version of ExaDigm Integrator software available for installation to Merchant terminals in a timely manner upon implementing the security updates, payment industry compliance updates and enhancements to application features or functions.
- Maintain PCI PA-DSS compliance for all newly released software versions.
- Maintain the integrity of software release by enforcing secure software authentication policies. All ExaDigm Integrator software is delivered securely according to strict PCI PA DSS requirements.
- Notify Customers about new version releases.
- Maintain detailed documentation, such as release notes, implementation guide, user guide, outlining all changes in functionality of software with focus on configuration of security features of the software.

ExaDigm makes the most current software available to all customers via the ExaDigm support portal. The ExaDigm N5 has an Update function where the user can simple press to update the latest firmware and or associated apps. The Exadigm N5 will also update itself when rebooted and also every 24hours automatically.

9.8.2 Customer Control Responsibility

It is the customer responsibility to initiate a software update by following the detailed instructions specified in the ExaDigm Integrator User Guide and/or provided above.
Note: perform all settlement functions prior to code update. In order for you to maintain your PCI DSS compliance, you must take steps to retrieve and update your ExaDigm Integrator application when contacted.
Contact ExaDigm customer services at support@exadigm.com to obtain the most current software version and to learn more about ExaDigm products.

9.9 PA-DSS Requirements 10.1, 10.2.3, and 12.1 (12.1.1)

Software vendor must facilitate secure remote access to payment application.

9.9.1 Software Vendor Control Responsibility

ExaDigm Integrator does not support remote access. N5 terminals do not have any services facilitating remote access. ExaDigm will only provide phone support.

9.9.2 Customer Control Responsibility

One may install one's own system for remote access capabilities, but in order to maintain PCI DSS compliance only remote access technology supporting multi-factor authentication must be used. Multi-factor authentication consisting of something you have, know, or are is required for remote access in order for you to maintain your PCI DSS compliance. In addition to the use of multi-factor authentication, it is important to remember that the remote access capability should only be enabled when needed and disabled when no longer required. Furthermore, your remote access software must provide for the following features or configuration settings:

- One must ensure changes are made to the default setting in the remote access software;
- Remotes access software must be configured to only allow access from specific IP addresses;
- Encrypted data transmissions such as IPSEC VPN, SSH, TLS or must enforced;
- Access to customer passwords must be restricted to authorized personnel;
- Logging of remote access must be enabled;
- Systems must be configured so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed;
- Unique user IDs must be used for each user account;
- Authentication composed of passwords and two-factor authentication must be used for remote access;
- Remote access must not require or use any group, shared, or generic accounts or passwords;
- Passwords must change every ninety (90) days or less;
- Passwords must be a minimum of seven (7) characters;
- Passwords must contain both numeric and alphabetic characters;
- Password history of the last four (4) passwords must be kept and new passwords must be different than any of the last four (4) passwords;
- Account lockout must occur after six (6) invalid logon attempts;
- Remote access accounts must be locked out for no less than thirty (30) minutes or until reset by a system administrator; and
- Remote access sessions must timeout after no more than fifteen (15) minutes of inactivity.

Note: All remote non-console administrative access to the systems in the environment must be encrypted utilizing SSH, VPN, TLS or other encryption technology in order to maintain PCI DSS compliance.

9.10 PA-DSS Requirements 11.1 &11.2

Software vendor must facilitate secure transmission of cardholder data across public networks.
Software vendor must facilitate secure use of end-user messaging technologies (for example, e-mail, instant messaging, chat) for transmission of cardholder data.

9.10.1 Software Vendor Control Responsibility

The ExaDigm Integratoruses TLS 1.2 for transmission of all cardholder data across any network type. This is by default and does not require you to configure anything. The application will only connect to processor sites with a valid site certificate. If the application cannot validate the processor's site certificate, it will generate a connection failed error and you must contact your processor and instruct them to install a valid certificate.

The ExaDigm Integrator does not support end-user messaging technologies (such as e-mail, instant messaging, chat) for transmission of cardholder data.

9.10.2 Customer Control Responsibility

ExaDigm advises the merchants on following, if they plan to use above mentioned end-user messaging technologies:

- Establish procedures for using the secure solution to render the PAN unreadable or secure the PAN with strong cryptography.

- Establish instruction that PAN must always be rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies.

9.11 PA-DSS Requirements 12.1 and 12.2

Software vendor must facilitate secure non-console administrative access and support multi-factor authentication for non-console administrative access.

9.11.1 Software Vendor Control Responsibility

The ExaDigm Integrator does not support non-console administrative access.

9.11.2 Customer Control Responsibility

Although the ExaDigm Integrator application and N5 terminals do not support non-console administrative access, if you decide to support non-console, administrative access to systems deployed in the same environment as the ExaDigm Integrator application, said access must support the following for your own PCI DSS compliance status:

1. Remote administrative non-console access must be secure with strong-crytography.
2. Remote administrative non-console access must support multi-factor authentication.

How the two requirements are met within your environment is dependent upon the technology you chose to support said access.

10.0 Appendix A: Software Version Management System

All software source code files and corresponding documentation are to be preserved in the Software Version Management System Database. ExaDigm employs the Git version control system. Access to source code is restricted by user name and password. User names and passwords are assigned by the Access Administrator. This measure ensures that only authorized personnel have the ability to make changes to the source code base. The Access Administrator is notified by the Human Resource manager regarding termination of employment and takes action to disable access by former employees.

10.1 Application Version Numbering

A new version of the custom Application is written based on the latest released version of the Integrator Application Framework in accordance with *PA-DSS Program Guide*. Payment Applications have separate naming and versioning conventions, and the Integrator Application Frameworkhas a separate versioning convention.
The Integrator Application Framework version has the format "XX.YY.ZZ" and is assigned by the CTO according to the following rules:

- First two digits "XX" represent the "Major" version number, i.e. "01". Major version represents the version of the main branch. It is increased only, if changes were made to the application's external interfaces, such as Shared Objects API or inter-application API, if the new version is a result of a merge of multiple offspring branches, if a security flaw was found or if the key management technique was modified as required by PCI PA-DSS.
- Next two digits "YY" serve the purpose of tracking the branches and minor releases. Branch can be opened to start the parallel development based on the previously released version of Integrator Application Framework.
- The final two digits "ZZ" represent minor revision started due to bug fixing after software was published. I.e. "01.10.02" is a second minor revision of the branch version "01.12". Minor Revision version ZZ is increased if the release is a result of correction of the defect reported by customer.

Versions should not be changed during internal Development-Testing iterations between QA and Engineering. If a new Application is written, it must be given a unique name according to the ExaDigm Naming Convention described in the document "Application Naming Convention". Importing the application with the same name and version as one of an existing applications will result in an error to prevent overwriting the previous application. The software versioning process does not support the use of wildcards in any position for any reason.

11.0 Appendix B: General Deployment Summary

This guide provides details that define how to properly deploy the ExaDigm Integrator application within your environment to help you achieve PCI DSS compliance.
Following the guidelines within this guide does **NOT** make you PCI DSS compliant, nor does it guarantee your network's security. It is your responsibility to ensure that your hardware and network systems are secure from internal as well as external threats. While this guide will go over the requirements you will need to follow for the implementation of the ExaDigm Integrator that will help you achieve PCI DSS compliance, it is your sole responsibility to ensure the proper implementation of the application.

Exadigm makes no claims on the security of your network, nor of your level of PCI DSS compliance.

The ExaDigm Integrator application comes pre-deployed on a PCI PTS approved N5 POI Terminal. All required PCI/PA DSS related features are enabled and specifics may be found in this guide for each PA DSS requirement section.
Upon receipt of your device, you will need to power on the terminal and connect it to your network. This device is to be placed within an internal network and is not to be placed in a DMZ zone or network.
The application has PCI DSS required logging enabled by default and this cannot be disabled or modified. The application supports the ability to export logs to a USB drive that you insert into the terminal. The process for doing this is found in Section 4.1 and 4.4 of this guide.
The application automatically encrypts data and does not require you to take steps to enable this feature. The keys for data encryption change automatically following the DUKPT key management scheme. See PA DSS 2.1, 2.2, and 2.3 & PA DSS 2.4, 2.5, 2.5.1 – 2.5.7 & 2.6 section for more details.
The application is configured by default to never display the full PAN. This cannot be modified by you. The application is configured by default to talk to your processor over a TLS 1.2 connection and cannot be disabled. Please see the general user guide for entering your merchant information.
Neither the ExaDigm Integrator application nor the supported terminals support remote access or non-console administrative functions. This is not a feature that is within the application or hardware and it cannot be added. You may decide to implement remote access for your environment, but you must do so in a PCI DSS compliant manner. Guidance can be found in PA DSS section 8 and 10 of this guide.
The ExaDigm Integrator application operates on a wireless N5 terminal. When you setup the application and terminal, you will be prompted for WPA2 password. Neither the terminal nor theExaDigm Integrator application will connect to an insecure wireless network. Guidance on wireless networks can be found in PA DSS section 6.

This page intentionally left blank.

12.0 Appendix C: Typical Network Implementation

An N5 terminal running the ExaDigm Integratoroperates on a Merchant's Local Area network. It is the Merchant's responsibility to maintain the LAN in a secure fashion compliant to PCI DSS requirements. Although N5 terminal are not servers, it is ExaDigm’s responsibility to remind a merchant that, according to PCI PA DSS requirement 9.1, merchants must not store cardholder data on servers directly connected to the Internet. It is mandatory to have an active firewall installed in the office or store. N5 terminals with the ExaDigm Integrator application communicate to Payment Processors or Gateways over the Public Internet utilizing TLS 1.2 secure Internet protocol to protect the payload of transactions. A typical production environment uses port 443 for communication to a payment processor. This must be allowed outbound on your firewall. There is no communications between deployed N5 terminals within the same network or other networks.

The ExaDigm Integrator application only operates on the following terminal type:

- ShenZhen Xinguodu Technology Co. Ltd PCI PTS POI device: N5

The defined terminal runs a vendor proprietary OS based on Android 5.1.1 (Lollipop) There is no additional services, protocols, components, hardware, or software beyond what is defined above.

13.0 Appendix D: 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 every merchant/service provider should adopt in developing and implementing a security policy and program:

1. Read the current version of the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.
2. Once 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.
3. Create an action plan for on-going compliance and assessment.
4. Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self-Assessment Questionnaire.
5. Call in outside experts as needed.

<<<END OF THE DOCUMENT>>>