新国都	FILE NAME	**PCI Security Policy for G3N**		
	FILE NO.			
PCI&PIN	VERSION	V1.11	CLASS	PUBLIC

PCI Security Policy for G3N

AUTHORIZER	AUDITOR	AUTHOR
PXB	PXB	GHZ

FILE NAME		**PCI Security Policy for G3N**			
CLASS		PUBLIC	FILE NO.		
No	VER	DATE	REVISION	AUTHOR	AUDITOR
1	1.01	2014/10/18	Create	GuoHongzhi	PengXuebing
2	1.06	2014/12/25	For G3 OP descript	HuangLing	GuoHongzhi
3	1.08	2016/01/21	For G3 MIS descript	PengHuanjie	GuoHongzhi
4	1.09	2016/8/10	For G3N Terminal	PengHuanjie	GuoHongzhi
5	1.10	2016/9/27	For G3N Terminal New Panel	PengHuanjie	GuoHongzhi
6	1.11	2016/10/26	Remove Copyright description	PengHuanjie	GuoHongzhi

CONTENTS

1 Introduction

This document describes the basic security policy for XGD POS device. It is used to guide product users and developers utilizing the security features more properly.

This document complies with the current security standards.

2 Scope

This documentation is applicable for XGD POS terminal and will be only released for trusted developers, testers, internal users and end users.

3 Acronyms

Abbr.	Description
TDES	Triple Data Encryption Standard
SHA	Secure Hash Algorithm
RSA	Rivest Shamir Adelman Algorithm
DUKPT	Derived Unique Key Per Transaction
PIN	Personal Identification Number
PED	PIN Entry Device
MSR	Magnetic Stripe Reader
ICC	Integrated Circuit Card
POS	Point of Sale
TRSM	Tamper Resistant Security Module

4 Reference

[1] X9 TR-31 2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms

[2] ANSI X9.24-1: 2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

[3] ANSI X9.24 Par2: 2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys

[4] ISO 9564-2, Banking —Personal Identification Number(PIN) management and security Part 2: Approved algorithms for PIN encipher

[5] PCI PTS POI Derived Test Requirements V4.0 – June 2013

5 Security Policy

5.1 Product Overview

G3N is a POS device which consists of a LCD display, a physical keypad, MSR, and ICC reader. The communication interface includes RS232 and USB. The picture is shown as below:

Figure 1 – G3N

5.2 Product Identification

The product name and hardware version are printed on a label on the device. The HW version can be identified from this label. Please see below picture (see red circle).

Figure 2 – G3N Identification

The firmware version can be checked via software menu.

(1) Access main menu by pressing “ENTER” when device power on.
(2) Select “5. Advance” to entry the sub-menu.
(3) Select “1.View FW Version” menu item to see the firmware version, for G3N, the FW version is “0258G3V404”.

5.3 User Guidance

This chapter mainly introduces how to use this device securely.

5.3.1 User Guide

The end user should check if all items are intact when he receives the device at the first time. The items along with the device include a G3N device, a battery, a power supply, communication cable and a copy of user guide specification. Before using this device, user needs to check if it is genuine and ready for use (Please refer chapter 5.3.5). If anything is lacking or damaged, user should contact with the vendor for inspection, refunded or exchange

5.3.2 Secure Usage Environment

This device is designed to be used in an attended environment.

The device only can work normally under a specific environmental condition. When the device detecting an abnormal condition existed, a tamper event will happen and all the sensitive information will be erased.

If the environment temperature is out of range (higher than 105°C or lower than -50°C), a tamper event will happen.

5.3.3 Device Design for Handheld

G3N terminal is a handheld POS device and has following features.

(1) With a battery which can be charged when necessary.
(2) Be able to enter power-saving mode when necessary.
(3) The housing is designed for handheld, which conform to human engineering in design.
(4) The weight and size are designed according to handheld device standard.

5.3.4 PIN Entry Guide

The G3N is handheld POS, Please note, If the device is in use of an unapproved method will violate the PCI PTS approval of the device.

The G3N is a handheld POS terminal which has no shield and printer. The customer should care to cover the key area with his (or her) hands and body during PIN entry. In this way, the digital keypad area will not be seen except the user and the PIN is protected from being revealed, as shown in figure 3.

Figure 3 – G3N PIN Input

5.3.5 Device Periodically Checking

The merchant or acquirer must visually inspect the terminal when received via shipping. The merchant or acquirer should inspect the terminal to ensure that:

(1) The merchant or acquirer should daily check that the terminal is not destroyed or installed a suspicious bug. Make sure the used devices are the approved ones.
(2) There is no suspicious wire being connected to any ports of the terminal.
(3) Hardware version and firmware version on terminal label or screen are consistent with the approved HW and FW version.
(4) There is no visible open case evidence via inspecting the device shell or the labels in screw holes.
(5) There is no suspicious thing appearing in ICC and MSR reader.
(6) The merchant or acquirer should also check that the installation/maintenance operations are performed by a trusted person.

The checking routines are applied for shipment or daily periodicity checking.

5.3.6 Secure Use ICC

To make sure IC card being used securely, the merchant should do the following inspections.

(1) Check whether IC card reader has a suspicious line. If yes, please stop using the device and inform the manufacture for security inspection.
(2) Check whether IC card can be inserted smoothly. If there is something blocking the card, or if the card can't be inserted into the slot normally, please stop using the device and inform the manufacture for security inspection.
(3) Check whether the shell of IC card reader interface is integral. If some damage evidences are found, please stop using this device and inform the manufacture for security inspection.

5.3.7 Secure Use MSR

To make sure MSR being used securely, the merchant should do the following inspections.

(1) Check whether the MSR slot has a suspicious line. If yes, please stop using the device and inform the manufacture for security inspection.
(2) Check whether the card can be swiped smoothly. If no, please stop using this device and inform the manufacture for security inspection.
(3) Check if there is any addition beside the MSR slot. If yes, please stop using this device and inform the manufacture for security inspection.
(4) Check whether MSR slot is destroyed. If yes, please stop using this device and inform the manufacture for security inspection.

5.3.8 Dealing with Fault

The merchant or acquirer should always concern the status of the device being used. Devices which are locked or display abnormal prompt must not be used for PIN transaction any more. When a tamper event occurs, the device must be inspected by the vendor. Users are advised to contact with vendor for further and detail secure inspection.

5.3.9 Procedures for Decommissioning Device

If the devices would be decommissioned permanently from service and no longer in use, they are gathered by secure man and erased all the key information. This can be done by taking the device apart to make it tampered or using a dedicate tool to delete the all the sensitive information. Then these devices are mandatory transported back to XGD factory for disassembling and recycling.

If the device requires a temporary removal, it is unnecessary to change the state of the device due to all the

sensitive information in the device are still under the protection of physical and logical protection mechanism.

5.4 Hardware Security

The device has tamper mechanisms that will trigger when a physical penetration attempt of the device is detected. Also it contains anti-detected mechanism to protect the device from being attacked.

5.4.1 Tamper Response Event

A merchant or acquirer can easily find a tamper event happen in the terminal. A flashing warning message is displayed on the screen and the terminal is locked when the device is tampered. All the sensitive data are erased and no one can use it again. Any tamper event happened will make the device out of normal service. The device has 2 separate modes as below:

1. Activated mode: the device is fully operational.
2. Freezing Mode: the device is tampered and can't be operated. It requires reactivation after maintenance and security inspection.

It should be mandatory to send the device back to the vendor for security checking and repairing when the device is tampered.

5.4.2 Environmental Failure Protection

The security of the device is not compromised by altering the environmental conditions (e.g. the temperature or operating voltages outside the stated operating range does not alter the security).

5.5 Software Security

5.5.1 Software Development Guide

The developers must accept training course before development activity starting. And they also need to obey the coding rules and best practices during the whole development stage.

5.5.2 Firmware and Software Update

When downloading or updating firmware or application, it needs authentication. XGD terminals only accept the firmware and software with legitimate and correct signature. The software and firmware loading process does not need to be protected by any special way. The device will reject to load and save any unauthenticated software and firmware.

Note that tampered devices will appear to be disabled, and will not allow software and firmware for running even if they are authenticated.

5.5.3 Firmware and Software Authentication

This device implements asymmetric cryptographic algorithm for firmware authentication. RSA algorithm with 2048bits key is used for signature verification and SHA256 algorithm is used to calculate the digest of firmware.

The firmware is signed by RSA-2048 bits private key which is only controlled by XGD. And the firmware authentication is executed by signature verification using corresponding public key of XGD.

Before firmware and application being executed every time, their integrity and validity will be checked. If it is failed, the terminal will not work correctly.

The certificate and signature of the application and firmware code are verified. The certificate and signature are based on RSA key pairs.

5.5.4 Key Checking

All keys stored in the device will be checked when power on or before being used every time. If the checking is failed, all the keys will be erased. When injecting keys, it needs to do authentication firstly.

5.5.5 Self-Test

Self-test is routinely executed upon start up or reset every time. This checking is also performed periodically (once a day) during the period of normal use. This test is not initiated by an operator.

5.6 System Administration

5.6.1 Configuration Settings

The device is functional when it is received by the merchant or acquirer. No security sensitive configuration settings are necessary to be tuned by the end user to meet security requirement.

5.6.2 Default Value Update

The device is functional when it is received by the merchant or acquirer. The default passwords for sensitive function management should be changed mandatorily when this device is used for the first time.

5.7 Key Management

5.7.1 Key Management Techniques

G3N POS terminal key management complies with ANSI X9.24 and TR-31 key management rule strictly. Each key has only one purpose and only one value. When the terminal is suffering attack, the keys are erased, which make the device more security.

G3N terminal implements different types of key management techniques:

Fixed Key: a key management technique based on a unique key for each terminal

Master Key/Session Key: a method using a hierarchy of keys. The session keys are unique per transaction.

DUKPT:a key management technique based on a unique key for each transaction

Please Note: Use of the POI with different key-management systems will invalidated any PCI approval of this POI.

5.7.2 Cryptographic Algorithms

G3N POS terminal can support the secure algorithm as following:

Algorithm	Size (Bits)	Remark
SHA-256	-	Integrity verification
Triple DES	112/168	Data encryption/decryption
RSA	2048	Data encryption/decryption, sign and verify signature

5.7.3 Key Management

RSA certificates are used in this device. The key sizes are 2048 bits.

Key Name	Purpose/Usage	Size (Bits)	Storage
SUPER ROOT PK	Authenticate the legitimacy of UBOOT when start up	2048	Embed in code
XGD ROOT PK	Authenticate certificate and firmware	2048	Embed in code
XGD PK	Authenticate certificate	2048	Secure Unit

KERNEL PK	Authenticate firmware	2048	Secure Unit
FSIMG PK	Authenticate firmware	2048	Secure Unit
XGDAPP PK	Authenticate certificate	2048	Secure Unit
ACQUIRERP PK	Authenticate application and certificate	2048	Secure Unit
MUTUAL AUTH PK	Verify identity authenticity	2048	Secure Unit

The transaction related keys are classified as following description. The algorithm used by following keys is TDES. These transaction keys (except Future DUKPTK) are controlled and generated by acquirer. All keys loaded into the device can't be obtained from external and exported to external by any way. These keys only can be used as the intended purpose via the interface or commands provided by the device.

Key Class	Key Name	Purpose/Usage	Size (Bits)	Storage
Main Key	TK_PIN	Key Encryption Key. Only used for unfold and install the cipher working keys (PINK and MACK).	112	Secure Unit
	TK_MAC		112	Secure Unit
Working Key	FIXEDK	PIN Encryption Key. Used to encrypt PINBLOCK.	112	Secure Unit
	PINK	PIN Encryption Key. Used to encrypt PINBLOCK.	112	Secure Unit
	MACK	MAC Encryption Key. Used to encrypt MAC value.	112	Secure Unit
Initial Key	Initial DUKPTK	Used to generate future DUKPT key	112	Temporary buffer
Working Key	Future DUKPTK	Online PIN Encryption. Used to encrypt online PINBLOCK.	112	Secure Unit

5.7.4 Key Injection Method

The device does not propose manual cryptographic key entry. Also, this device is not applied for remote key loading. Specific tools, compliant with key management requirements, shall be used for key injection.

The RSA key pairs are generated in a TRSM or secure PC, and these public keys are signed by proper secret keys. These operations are controlled by secure manager and happened in a secure room.

Initial keys should be loaded into the device by two trust person using an authentic key loading dedicated tool (TRSM or Secure PC) in secure environment. Certainly, dual control and knowledge split technology will be used during this key injection process. Only both the two correct passwords can enter TRSM system. Any 5 times error input password will cause all the keys gone and TRSM get back to initial status.

In MK/SK system, the working keys loaded into the device in the form of cipher, under the protection of main key.

5.7.5 Key Replacement Policy

Any key should be replaced with a new key whenever the compromise of the original key is known or suspected. If a tamer event has happened, the device is mandatory asked for secure inspection and sent to Key Authorization Center to inject new key again. The new key are injected via high secure channel (TRSM and secure communication path) and stored by encrypted method. Nobody can get these keys' information. This terminal implements tamper-detection mechanism and limits the use time of the sensitive service function. So it is infeasible to determine the keys through exhaustive attack elapses.

5.7.6 Key Removal

After keys being injected into device successfully, there are two ways to remove the keys. One is passively erased by firmware or hardware, like a tamper event happened. The other is actively cleared by secure manager via dedicate tool, like repair on request or decommissioning event happened.

5.8 Roles and Services

The device has no functionality that gives access to security sensitive services, based on roles. Such services are managed through dedicated tools, using cryptographic authentication.