新国都	FILE NAME	**PCI Security Policy for G2**		
	FILE NO.			
PCI&PIN	VERSION	V1.05	CLASS	PUBLIC

PCI Security Policy for G2

AUTHORIZER	AUDITOR	AUTHOR
CLL	PXB	LH

FILE NAME		**PCI Security Policy for G2**			
CLASS		PUBLIC	FILE NO.		
No	VER	DATE	REVISION	AUTHOR	AUDITOR
1	1.00	2017/02/20	Create	PHJ	GHZ
2	1.01	2017/09/09	Add work condition description	PHJ	GHZ
3	1.02	2017/09/29	Add OP/SSL description	PHJ	GHZ
4	1.03	2017/12/30	Add remote update	PHJ	WZC
5	1.04	2018/07/03	Change to the correct key length	CLL	LH
6	1.05	2018/07/04	Add SRED	CLL	LH

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 Components

5.1 Product Overview

G2 is a handheld device which consists of a LCD display, a physical keypad, MSR, and RF, ICC reader. The communication interface includes USB, GPRS, the pictures are shown as below:

Figure 1 – G2

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).

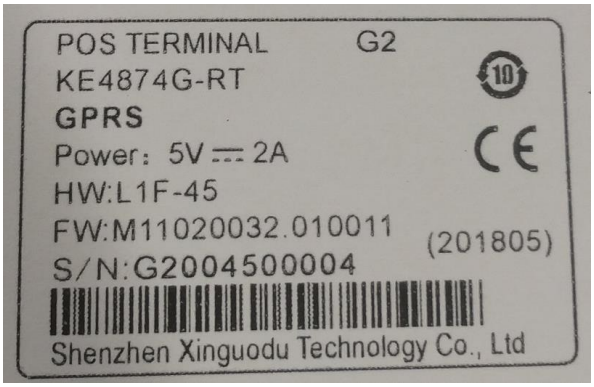

Figure 3 – G2 Identification

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, the FW version is

“FW: M11020032.010011”.

5.3 User Guidance

This chapter mainly introduces how to use G2 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 G2 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

G2 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

The G2 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

Please note, if the device G2 is in use of an unapproved method will violate the PCI PTS approval of the device.

For The G2 is a handheld POS terminal, it has no shield, so 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 5.

Figure 5 – G2 PIN Input

5.3.5 Device Periodically Checking

The merchant or acquirer must visually inspect the G2 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 tru sted 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 G2 would be decommissioned permanently from service and no longer in use, they will first be disassembled and enter triggered status, so as to erase sensitive information. Then these devices are mandatory transported back to XGD factory for disassembling and recycling.
If the G2 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 G2 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 happened in the G2 terminal. A flashing warning message is displayed on the screen and the terminal is locked when it is tampered, and the screen will be as figure 6 or figure 7. 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:

- Work mode: the device is fully operational.
- Lock 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.

Figure 6

Figure 7

5.4.2 Environmental Failure Protection

The security of the G2 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).
Working temperature range: 0℃～50℃(32℉～120℉)
Working humidity range: 10%～90%
Operating voltages：DC 5V

5.5 Software Security

5.5.1 Software Application 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.
The software programmers should not keep the user information (as PAN, etc…) in terminal longer than it really need, after used it should be cleared.
For the programmers of op application, he or she should keep the services as minimum as possible, and close the ports which are not used, to avoid disclosure of information or malicious attacking.
For the programmers of SRED application,
(1) All data involving the plaintext of the account data shall not be disclosed in any plaintext (including display on the terminal, plaintext transmission) to the account data;
(2) The account data is sensitive data and should not be stored in the application clear text data. After using the account data, the account data cache should be cleared immediately;
(3) The application does not allow the clear text data of the account transfer to other applications;
(4) For all application development codes, relevant personnel should be organized to conduct code reviews to ensure that the application code has correctly processed the plaintext of the account data;
(5) All application programs must be signed after confirmation, and can be downloaded to the terminal only after the terminal has been verified by the terminal.
The more information and notes please refer <Software Development Control Program.docx>.

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 Application Sign & Authentication

This device implements asymmetric cryptographic algorithm for firmware and application authentication. RSA algorithm with 2048bits key is used for signature verification and SHA256 algorithm is used to calculate the digest of firmware and application.
The firmware and application are signed by RSA-2048 bits private keys which are only controlled by XGD, and their authentication are executed by signature verification using corresponding public keys 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 firmware and application code are verified. The certificate and signature are based on RSA key pairs.

5.5.4 Application Test and Release

For the application to be released, should perform the steps of reviewing, testing and signing, to confirm its safety.

Review the code to make the program to be sane and security. the test flow to make sure the program`s function are good, and can be sane. The signing to confirm the application`s integrity, and can`t be tampered.

5.5.5 Key Checking

All keys stored in the G2 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.

5.5.6 Self-Test

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

5.5.7 Signature Mechanism

XGD use a signature system based on web server technology to sign and manage all files. This system implements a serial of important functions such access control, permission management, file signature, log management and etc.
A pair of signature operators will be granted and permitted to login this system and do signature operation. Only both of them are identified by the system (through entry respective passwords successfully) during a window time, they can use the signature function to sign firmware or application.
During the whole signature process, private key always remains in the encryption machine and never be exported. Only signed file will be output to outside. Certainly, any operation trace will be recorded by this system to make it more secure.

5.6 System Administration

5.6.1 Configuration Settings

The G2 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 G2 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

The G2 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. If the terminal is suffering attack, the keys will be erased immediately.
The G2 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
AES Key: a key management technology, used for **PINBLOCK format 4** encrypt algorithm.
Please Note: Use of the G2 with different key-management systems will invalidated any PCI approval of this POI.

5.7.2 Cryptographic Algorithms

The G2 POS terminal can support the secure algorithm as following:

Algorithm	Size (Bits)	Remark

SHA-256	256	Integrity verification
Triple DES	112/168	Data encryption/decryption
AES	128/192/256	Data encryption
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
Authority PUBLIC Key	Public key Authenticate when the TRSM and POS terminal, so as to inject keys.	RSA-2048	Secure Unit
SUPER ROOT PK	Authenticate the legitimacy of UBOOT when start up	RSA-2048	Embed in code
XGD PK	Authenticate Boot, xgd.pk, kernel.pk, fsming.pk, xgdapp.pk	RSA-2048	Secure Unit
KERNEL PK	Authenticate Kernel	RSA-2048	Secure Unit
FSIMG PK	Authenticate FS Image	RSA-2048	Secure Unit
XGDAPP PK	Authenticate Application	RSA-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、MACK、TDK).	AES-256	Secure Unit
	TK_MAC		TDES-168	Secure Unit
	TK_TDK		TDES-168	Secure Unit
Working Key	FIXEDK	PIN Encryption Key. Used to encrypt PINBLOCK.	TDES-112	Secure Unit
	PINK	PIN Encryption Key. Used to encrypt PINBLOCK.	TDES-112	Secure Unit
	PINK_AES	PIN Encryption Key. Encrypt PINBLOCK format 4.	AES-128/192/256	Secure Unit
	MACK	MAC Encryption Key. Used to encrypt MAC value.	TDES-112	Secure Unit
	TDK	PAN Encryption Key. Used to encrypt prime account data.	TDES-168	Secure Unit
Initial Key	Initial DUKPTK	Used to generate future DUKPT key	TDES-112	Temporary buffer
Working Key	Future DUKPTK	Online PIN Encryption. Used to encrypt online PINBLOCK.	TDES-112	Secure Unit

5.7.4 Key Injection Method

The G2 does not propose manual cryptographic key entry. Also, this G2 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.

Please Note: The original key must be replaced by a new key whenever it is revealed.

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 G2 has no functionality that gives access to security sensitive services, based on roles. Such services are managed through dedicated tools, using cryptographic authentication.

6 Update and Document Description

6.1 Local update

The device can be updated by managers or maintainers, the firmware & application be downloaded via USB disk, and the description documents will also be released on to the web site of company. These documents are all in PDF format, and were all signed by company, avoid being tampered or damaged.

6.2 Remote Update

The device support remote update. When there is any update to POS, manufacturer will release the new firmware and documents on its web site, and the manufacturer send mails to the managers or maintainers, and users, then the POS can be updated remote, no need send the devices to manufacturer again.

On the manufacturer, only the operation has permission, by its authority, the firmware can be put the signed firmware to server. And, only the valid device it has the correct public certificate, by it can connects to the update server, and get the updates. The connect to server will using TLS 1.2.

6.3 Update Responsibility

For the developer, they are the responsibility the offer firmware & documents, but do not perform update to device.

For the Integrator, he & she should take the updates from developer, and update the new firmware to server, for maintainers or users to get.

For the maintainers and users, they have the jurisdiction to connect the server and get the updates for devices.

7 Secure Reading and Exchange of Data

For the data reading & exchange in secure, the user should first inject the data key (TDK, it should be not less than 168 bits in TDES) for the device, this key will protect the data transmission in security. When in use, the plain data should be erased after encrypted immediately, and if the PAN need display to cardholder, only the first 6 and last 4 digits can be shown, other digits should be masked. The device is always in data security mode, and no method to change it to non-security mode.

Terminal does not support “pass-through of clear-text account data using techniques such as whitelisting”.

8 OP & SSL Using

For OP deploy, the user should refer to the released document <XGD PCI OP Interpretation.docx>.

Because of the vulnerability of SSL, so if use OP function, it should be removed.