Security Policy of xCL_RP-10

Version A05

Table of Contents

Revision History

Version	Comments	Author	Date
A01	Initial Release	Tony	2017/3/27
A02	Update key table	Tony	2017/10/25
A03	Update the table on Chapter2.1	Tony	2017/11/03
A04	Update HW version	Sean	2021/12/13
A05	Update Section 1.1	Sean	2022/01/21

1 Overview

This document which is a security policy of the device includes the use of device, key-management, responsibilities, device functionalities, and environment requirements.

1.1 Reference

The related documents which are referred by this document listed here:

[1] XAC Product Delivery A03.pdf

2 Device Description

This document is a security policy for xCL_RP-10 which includes the use of device, key-management, responsibilities, device functionalities, and environmental requirements.

The device is designed as a PED for supporting payment with PIN entry, and dedicated to payment; and completed meet all requirements of PCI PTS POI 5.1. Any deviation from the approved use of the device will invalidate the PCI PTS 5.1 compliance approval.

Device photo

2.1 Introduction

- Device Name: xCL_RP-10
- Hardware Version: R X 1 0 x 3 2 U H x G 7 F 4 0, R X 1 0 x 3 2 U H x x 7 F 4 0
- Firmware Version: 3550100x

Features & Functions	xCL_RP-10
LCM 2.4" + Touch	+ Touch
MSR	V
SCR	V
CTLS	V
Keypad + backlight	V/X
USB cable support	V

FW version will be showed on the LCM when the device is turned on.

The xCL_RP-10 is a PIN Entry Device with 2.4” touch display. Physical keypad (15 keys) is used for PIN entry.

The device is protecting by tamper detection and signing mechanism. The unauthorized function is not allowed by this device. Any unapproved use of xCL_RP-10 will result in non-compliance with PCI PTS POI security requirement.

2.2 Environmental Conditions

The device is designed for handheld POI.

2.2.1 Power

- Powered by USB type A cable (5V/500mA)
- Power adaptor : 5V / 2A
- Li-Ion Battery 3.7V /3100 mAH

2.2.2 Operating Condition

Temperature: 0°C to +50°C
Relative Humidity: 5% to 95% RH (non-condensing)

2.2.3 Storage Condition

Temperature: -20°C to +60°C
Relative Humidity: 5% to 80% RH (non-condensing)

2.2.4 Failure Protection

If the following conditions happened, it will trigger the tamper events.

- RTC battery (coin battery) voltage is above 3.6V or below 2V. (Maxim32552 detection)
- Operating temperature is above 70°C or below -20°C.

2.3 Device Information

2.3.1 Hardware Information

The label at the bottom of the device shows the hardware information as shown in the following figure.

2.3.2 Security Configuration Settings

The device is functional when it is received by the merchant or acquirer. No security related configuration settings need to be tuned by the end user in order to meet security requirements. The device is compliance with the SRED security standard, which means it will not output plaintext cardholder account data, such as Track 2 data. The data protection is built in for the device. There is no configuration to disable this security.

2.3.3 Default Value Update

The device is functional when it is received by the merchant or acquirer and there is no security related default value (e.g. admin password) that needs to be changed before operating the device.

2.4 Roles

The different operations on the device are defined as follows.

- Manufacturer: Top-level key injection.
- Administrator: Password modification and enable the transaction functions by performing installation process.
- Cardholder: Inputs the PINs.

The device will display non-significant characters while entered PINs.

3 Device Decommissioning

3.1 Introduction

This procedure describes how to decommission xCL_RP-10. While running decommissioning, it is necessary and important to remove all security data stored in the device.

3.2 Keywords

The description of some keywords, such as "Decommission Procedure", "Transfer" and "Proof". listed below.

Keyword	Description
Decommission Procedure	Have an assurance of removing sensitive data stored in the device (e.g. key) which cannot be recovered.
Transfer	Transfer means the change of ownership of devices. It may be from merchant to acquirer or acquirer to merchant.
Proof	A certified statement and/or a detailed log completed and signed by the person who supervised the decommission procedure.

3.3 Policy

1. Acquirer shall remove all security data before the device's transfer or removal from ownership.
2. All decommissioned device must follow a uniform and consistent method for the removal of security data described in this procedure.
3. Identify the device(s) to be removed from inventory or transfer from merchant before decommissioning.
4. Decommissioned device(s) will be labeled with a Tag indicating that security data has been erased from device.
5. All decommissioned devices will be documented/logged that tracks the serial number, signature and date.
6. Once decommissioning has been completed, there's no way to recover the erased sensitive data (e.g. key).
7. The person who supervises or executes the decommissioning shall provide name, title, and signature.
8. Make sure the decommissioned device is handled correctly.
9. It's even better to physically destroy the device after security data erasure, such as penetration of the keypad by special tools.

3.4 How to Erase the Security Data

Removing all security data stored in the device is necessary for all decommissioned device(s). The steps listed here for your reference.

1. Identify that if the device(s) is from inventory or is transferred from merchant and are prepared for decommissioning.
2. Power on the device
3. Open the housing to trigger device tamper.
4. Make sure the device is in tamper mode (the tamper message shown on screen can be checked to confirm that the device has tampered).
5. Power off the device

3.5 Decommission Record

Acquirer must retain a proof record of device decommission. At a minimum, the record has to provide below information:

- The store's name.
- The serial number of the device.
- The date of decommissioning.
- The method(s) used to destroy the media (e.g. tamper the device).
- The name, title, and signature of the person who supervised/executed the decommissioning procedure.

Merchant	Device SN	Date	Tampered or Not	Signature

4 Privacy Shielding

xCL_RP-10 is a handheld device and designed to be used in attended environment. All the three series should not be used as a desktop device. xCL_RP-10 will provide two use cases that one with the privacy shield and the other without the privacy shield. The Merchant can decide by their own to install the privacy shield or not.

4.1 Without privacy shield

This is a recommended use that the cardholder can use his own body or free hand to block the view of keypad that he is not overlooked when entering his PIN code.
It is a recommended use for entering the secret information by customer on this handheld device to avoid disclosing from intended or unintended sight. The following description will meet the PCI PTS POI DTR v5 appendix A.2 requirement.

(1) The cardholder can use his own body or free hand to block the view of the keypad, so that the PIN cannot be spied.

(2) The device can display a message for advising the user to position the device and shield the keypad while entering the PIN.

(3) Users need to rotate the keypad away from anyone who could be trying to spy their PIN.

(4) For PIN entry security, the notice items are described in the development document to guide customer that when user enters PIN, device will pop up a reminder.

(4.1) The description example of the reminder when entering PIN is as below:

"Shield your hand with a paper sheet or envelope or hand, and then enter the PIN code by using this way of protection."

(5) The device will also be pasted with a remind sticker:

4.2 With privacy shield

xCL_RP-10 also provides a privacy shield as an option for the Merchant. PIN entry can be confidentiality by this protection.
It is a recommended use for entering the secret information by customer on this handheld device. The following description will meet the PCI "Visual observation deterrents" requirement.

(1) The cardholder can use his own body or free hand to block the view of the keypad, so that the PIN cannot be spied.

(2) The device can display a message for advising the user to position the device and shield the keypad

while entering the PIN.

(3) User need to rotate the keypad away from anyone who could be trying to spy their PIN.

(4) For PIN entry security, the notice items are described in the development document to guide customer that when user enters PIN, device will pop up a reminder.

(4.1) The description example of the reminder when entering PIN is as below:

"Shield your hand with a paper sheet or envelope or hand, and then enter the PIN code by using this way of protection."

(5) The device will also be pasted with a remind sticker:

(6) Please see below photos of with a privacy shield:

xCL_RP-10

5 Key Management & Key Loading

All of the plain-text keys are loaded into device by manufacturer in key injection room. The others key encrypted by plain-text key can be loaded by acquirer or manufacturer. Either plain-text or chipper-text keys are managed under split knowledge and dual control.

5.1 Key Management Techniques

The device implements different types of key management techniques:

- 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 .

5.2 Cryptographic Algorithms

The device includes the following algorithms:

- Triple DES (112 bits and 168 bits)
- AES (128/192/256 bits)
- RSA (Signature verification, 2048 bits)
- SHA-256

5.3 Key Table

5.3.1 Keys under CPU

Key Name	Algo.	Size (bits)	Description / Usage	Storage
MRK	ECDSA	256	Authentication of CRK certificate	Stored in security processor ROM memory. Embedded in MAX32552 Bootloader
CRK certificate	ECDSA	256	Authentication of firmware modules	Programmed into security processor OTP memory
Flash memory Data Protection Key Flash KEK	AES	256	Encrypt all keys stored in internal Flash of security CPU.	Stored in plain-text inside NVSRAM of security processor.
XAC FW integrity check Public Key (PUK)	RSA	2048	Verify FW image.	Stored in plain-text internally in Flash memory of security processor.
Basic Key Loading Key (BKLK)	TDES	128	Encryption of the following keys for transmission to the device. (a) Master Key (b) DUKPT IPEK.	Stored in ciphertext inside Flash memory security processor.
Basic Key Loading Key Triple Length (BKLKT)	TDES	192	BKLKT is a KEK. used to load 16-byte or 24-byte TDES keys	Stored in ciphertext inside Flash memory security processor.
AES Basic Key Loading Key (BKLKA)	AES	256	BKLKA is a KEK used to load AES key	Stored in ciphertext inside Flash memory of security processor.
User defined non-volatile key	TDES	128 or 192	Encryption of the following keys for transmission to the device. (a) PIN encryption (b) Data encryption (c) MAC generation	Stored in ciphertext inside Flash memory of security processor.
DUKPT	TDES	128	The key used to generate UKPT. Slot “Z” is for PAN Encryption only	Stored in ciphertext inside Flash memory of security processor.

Key Name	Algo.	Size (bits)	Description / Usage	Storage
User defined volatile key	TDES	128 or 192	SK can be used for - MAC generation and verification - data encryption - account data encryption The acquirer may load multiple SKs (under encryption of MKs) for above purposes respectively.	Stored in plaintext internally in SRAM.
User defined volatile key (PAN Encryption Only)	TDES	128 or 192	SK can be used for - account data encryption	Stored in plaintext internally in SRAM.
TR-31 Key Block Protection Key (TR-31 KBPK)	TDES	192	TR-31 KBPK	Stored in ciphertext inside Flash memory of security processor.
TR31- DUKPT (TR-31 user DK)	TDES	128	The key used to generate UKPT	Stored in ciphertext inside Flash memory of security processor.
User defined non-volatile TR31 master key (TR-31 user MK)	TDES	128	TR-31 user MK is a KEK	Stored in ciphertext inside Flash memory of security processor.
User defined volatile TR31 session key (TR-31 user SK)	TDES	128	TR-31 user SK	Stored in ciphertext inside Flash memory of security processor.

Use of key management and keys other than those described in this document and related documents will invalidate any PCI approval of this POI.

5.4 Initial Key Loading

The device does not propose manual key and remote key injection. All initial keys shall be loaded into the device by the trustee using the authentic key loading device in secure environment.

The keys are managed under split knowledge and dual control by ensuring that multiple personnel who are required to undertake specific actions and respond to regarding effective key management procedures.

5.5 Key Replacement

If the merchant or the acquirer suspects anyone of the symmetric/asymmetric keys described in section 5.1 is known or compromised, the device shall be returned to the acquirer for key replacement. If the acquirer thinks that the time required for exhaustive attack to anyone of the symmetric/asymmetric keys seems feasible, it has to ask the merchants to return the device for key replacement too. The acquirer shall use its key loading facilities to replace the suspected key with a new and random value. It's better that the acquirer defines its own procedure for device returning and key replacement.

6 Signing Mechanism

6.1 Introduction

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. Digital signatures employ a type of asymmetric cryptography. For messages sent through a non-secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

6.2 Keywords

The description of some keywords of digital signature, like “Authentication”, “Integrity”, and “Non-repudiation” described below.

Keyword	Description
Authentication	When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user.
Integrity	If a message is digitally signed, any change in the message after signed will invalidate the use of the signature.
Non-repudiation	Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

6.3 Features

A digital signature typically consists of the following features:

1. A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
2. A signing algorithm is given a message and a private key, and then produces a signature.
3. A signature verifying algorithm is given a message, public key and a signature, and then either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key.

6.4 Signing Mechanism

The firmware which are using in the device will be signed by RSA key. The signing information allows the terminal (OS) to authenticate the legality of the update packages at installation time. This signing process is auditable and using high level security process (an example is using a Hardware Security Module), and requires dual control.

6.5 XAC Methods

The methods of digital signature used in XAC are listed below:

1. **FW update mechanism:**
   (1) The FW's SHA-256 hash is signed by Image Integrity Check (IIC) PRK, then the FW image is fragmented (2KB for one block) and scrambled before download.
   (2) The scrambled FW image is descrambled to recover after downloading.
   (3) Calculate SHA-256 hash of the FW
   (4) Use IIC PUK to decrypt the signed SHA-256 hash coming along with FW image.
   (5) Confirm (3) = (4).

7 Device Guidance and Maintenance

7.1 Installation Guide

The device is always shipped to customer with an installation guide. Following information is listed in the installation guide.

1. Power and cable connections information.
2. Communication ports information.
3. The main characteristics of the device (e.g. temperature, humidity, voltage, etc.)
4. Safety and security information.

7.2 Initial Inspection

It is recommended that to do the inspection after receiving goods via shipping.

1. The merchant or acquirer must visually inspect the terminal for the sign of tampering.
2. There are no unusual wires that connected to any ports, or MSR/ICC slot of the terminal.
3. There is no shim device in the slot of the ICC acceptor or nearby the MSR header
4. The keypad is firmly in place.
5. There is no overlay keypad on device.
6. The terminal serial number is corresponding to the inspection one.

Doing the checks would help to prevent any unauthorized modifications to or substitution of the terminal.

7.3 Procedure of Periodic Examination

The device should be kept in good condition for daily use, with below procedure being followed.

1. The merchant should check the appearance of the device every day for prevention of tamper through PIN-pad overlay. The ICC slot should be check every day for any abnormal imprint.
2. If the device keypad is non-functional, the device will turn off the display (as figure 7.1), This means the device is tampered
3. After updating the FW, the device will send out tamper message (as figure 7.1).

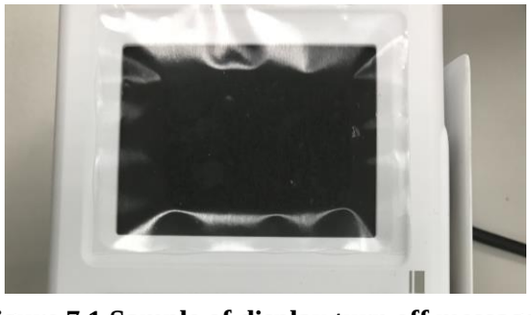

Figure 7.1 Sample of display turn off message

Figure 7.2 Sample of Tamper message

When the warning message is displayed on the device, the merchant should be educated to identify such tampered device, and shall return the device to the acquirer immediately.

7.4 Procedure of Periodic Maintenance

For secure operation of the device, the procedure below shall be followed.

1. The device shall be always in least privilege state for daily use.
2. The merchant should not change any setting of the device unless really required.
3. The acquirer shall deploy the updated OS/FW (or patches, etc.) to all the devices as soon as possible once he receives them from XAC.

7.5 Confidence Use of ICCR

The device is designed to be used in attended environment.
It's recommended that the merchant should take care that:

1. Inspect the device and make sure there are no unusual wires connected to ICC slot.
2. Inspect the device and make sure there is no shim device in the slot of the ICC acceptor.
3. While the transaction is using chip cards, the indicator of ICC slot would be lighting to green. If any abnormal happened (for example, the light is always off), please remove chip card from the device and contact your acquirer immediately.

8 Firmware Review Guidance

Security module firmware review procedure:

Scope:

This procedure is to define the review process of the firmware module for the security products.
(1) Source code back up,
The source code will be backed up in authorized controlled system to limit the accessibility.
(2) Reviewer assigned,
When a project is started, a reviewer will be assigned to the review the code which is released by the programmer.
(3) Review frequency,
The program under development should be released and reviewed every week after the coding is started.
(4) Review process,
When the programmer releases the on-going source code, a release form is attached. The reviewer will put the code into the system after reviewing the code and the release form. The reviewer will ensure that the programmer is releasing only those modules assigned to that programmer and that the additions and changes in the code are consistent with the release form information and the product requirements.

The audit trail consists of all the released modules and their associated release form. All released modules are retained such that at any time it is possible to go back and review again all the releases of any part of the source code.

9 Device Delivery

The guidance describes device delivery as following:

1. Secure packing.
2. Shipping record
3. The state of device.
4. The actions on receiving the goods.

Please refer to "XAC Product Delivery A03.pdf" for details.

10 Self Tests

Self-tests are performed upon start up and every 12 hours during the normal use of the device. And the device will reset every 24 hours. These tests are not initiated by an operator.

Self-tests include:

- Check of integrity and authenticity of the software.
- Check of the security mechanisms for sign of tampering.

If a self-test fails, the device halts all operations. If tamper are triggered, the device will erase the key register.

All keys are checking again by firmware each time before the key using. Firmware will check the key value and it’s KCV. Firmware will output an error message if check failed.

11 SW Update

For secure operation of the device, XAC provides update of FW. The update can be executed locally.

11.1 Local Update

1. XAC notifies the customer there's an update for some device.
2. The customer responds to XAC and prepares to receive the update.
3. XAC sends the encrypted update to the customer, or the customer downloads the encrypted update from XAC server.
4. The customer sends maintenance people carrying special devices to perform the update to all devices on-site.

All these updates will contain signature produced by XAC private key to ensure authenticity and integrity of the update at customer site. The device checks the signature after download of the update, and rejects the update if it finds incorrect signature.