Clover Mini Security Policy

## Table of Contents

## Introduction

This document addresses the proper use of the Point of Interaction Device (POI) in a secure fashion. This includes information about key-management responsibilities, device functionality, identification, installation, operating guidance, environmental requirements and administrative responsibilities. This document addresses the security requirements listed in DTR B20 of the PCI PTS POI Version 4.0 document. This device is vendor controlled and it is required that the vendor manage all payment security related functions.

## General description

1. Product overview
    a. Clover Mini (see image 1) is designed as a pin entry device (PED) to facilitate credit and debit based transaction. The device is only approved for use in an attended environment. This device has a color LCD with touch screen as the customer interface for PIN entry. The device also runs software to support the business operations of the owner.

Image 1

2. Device Functionality

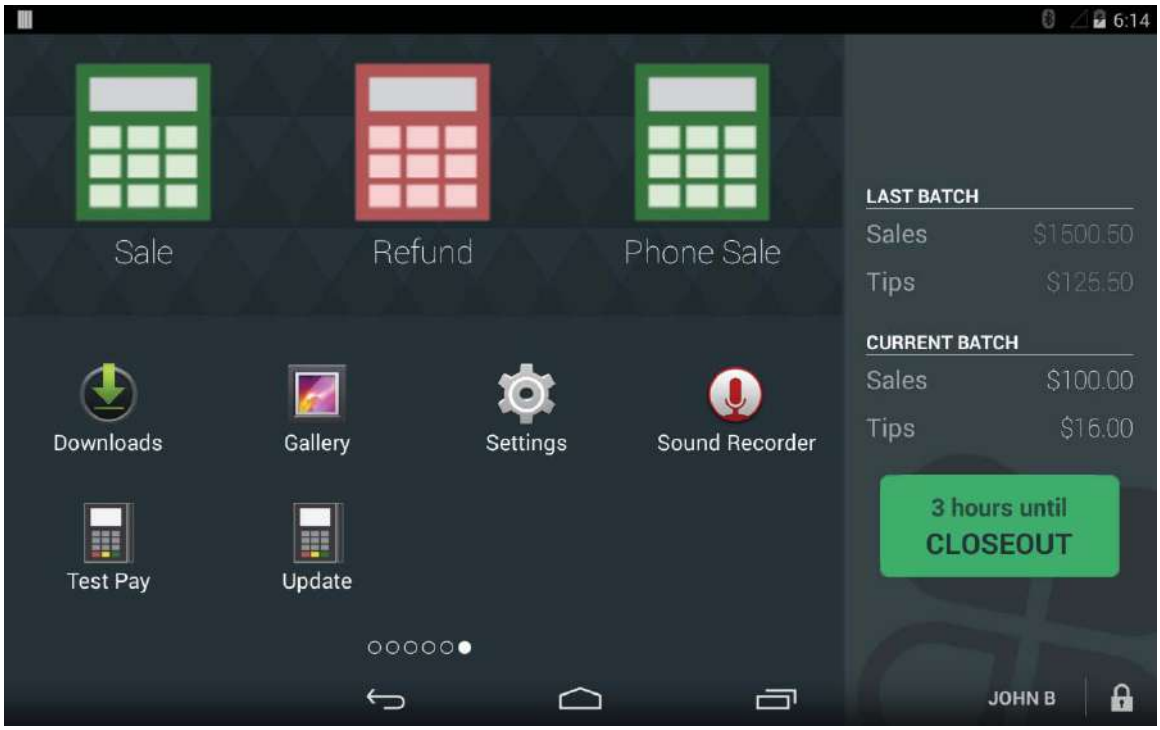
a. This device obtains card data via Integrated Circuit Card Reader (ICCR), Magnetic Stripe Reader (MSR), manually entered cards and Near Field Communications (NFC).
b. This device uses a Remote Key Injection (RKI) process to distribute symmetric keys used to secure transactions. There are no administrative modes available to the end user.
c. This device uses cryptologic authentication on all code before execution.

3. Device Identification
    a. Identifying information is presented on the label inside the printer as seen in Image 2 and 3.

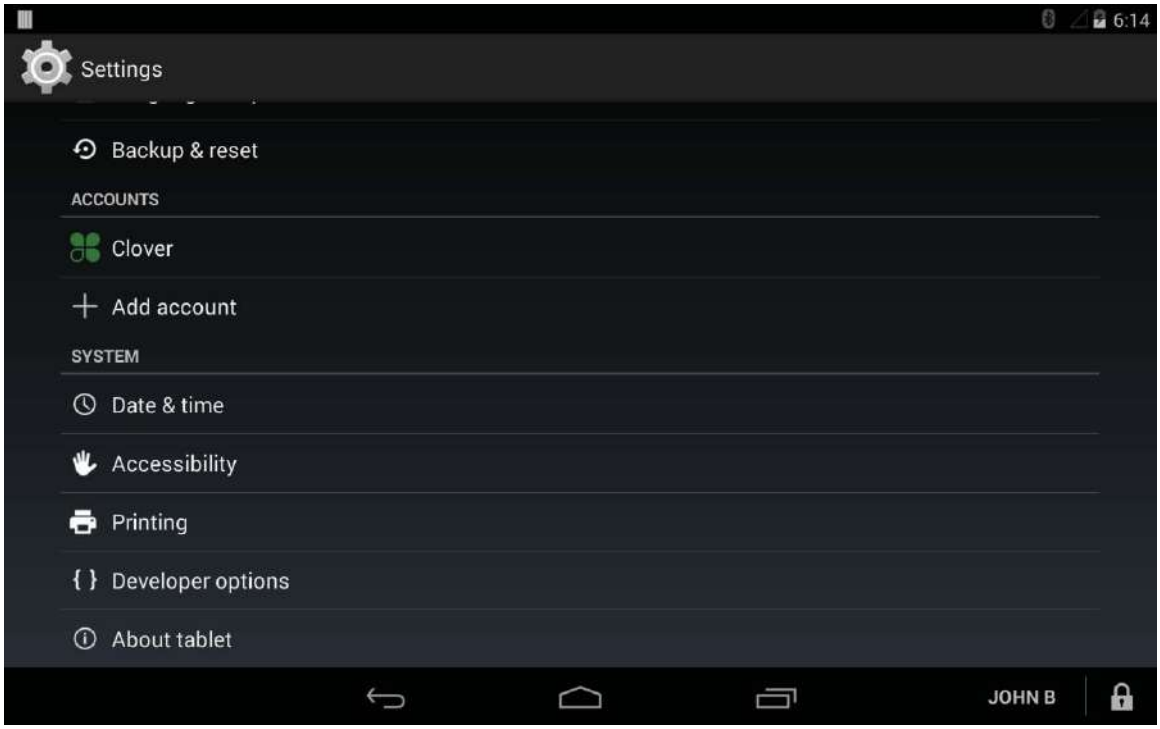

Image 2


**Image 3**

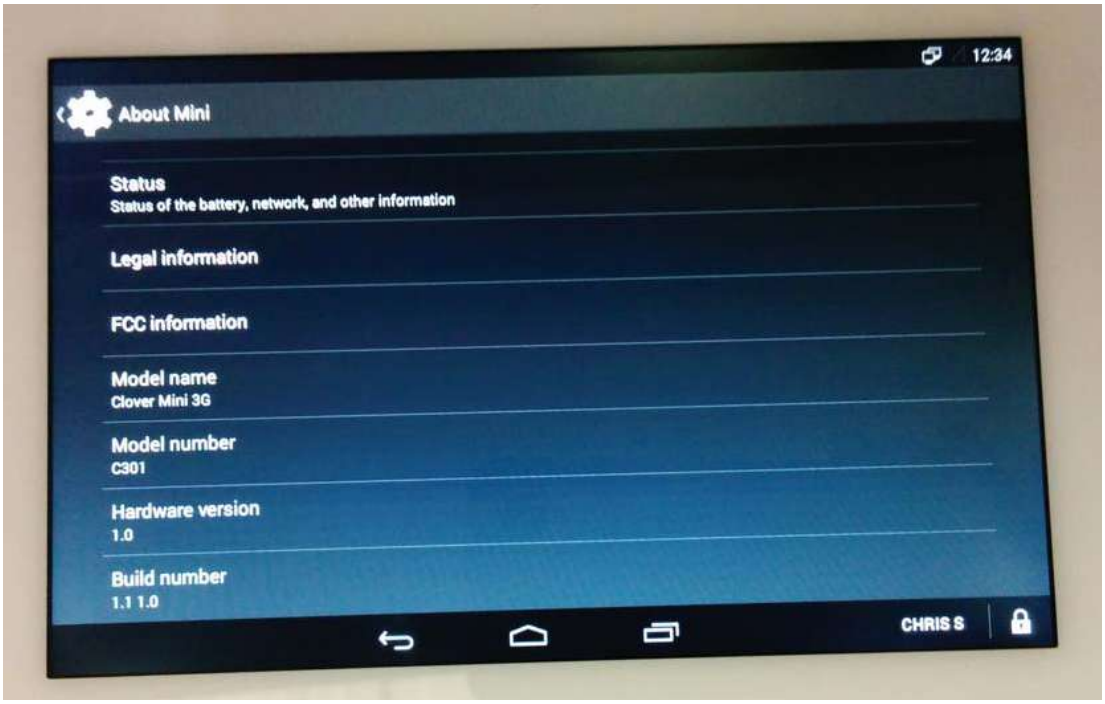
4. Version Information
    a. Software and firmware are displayed on the settings section on the device. The user should regularly check the software and firmware version of the device.
    b. From the main screen, click on “Settings”




c. Click on "About tablet"




d. View version numbers




## Installation Guidance

1. General Instructions
    a. Initial setup of the device is conducted by the end user and requires that user to have administrative rights to the merchant account. There are no additional roles required.
    b. Upon receipt of the device, the end user must connect the device to Clover's servers via an Internet connection. Any Wi-Fi connection must be encrypted. Merchants should use connectivity secure at a level equal or greater than WPA or WPA2.
    c. Once connected, the end user must enter a one-time security code provided by Clover. This code is communicated via a different communication channel than the device itself.
    d. Once the code is verified against the requesting device, the device shall perform security updates including injection of security keys. The end user is not required to perform any jobs necessary for security.
    e. Upon completion of setup, the end user may determine which additional employees will have access to the device. The end user must follow PCI security best practices when training additional users.

f. In addition to the device, the end user also receives
    i. A power adapter
    ii. A PIN Shield
    iii. An overview guide
    iv. A link to the help website where updated documentation and FAQs are stored

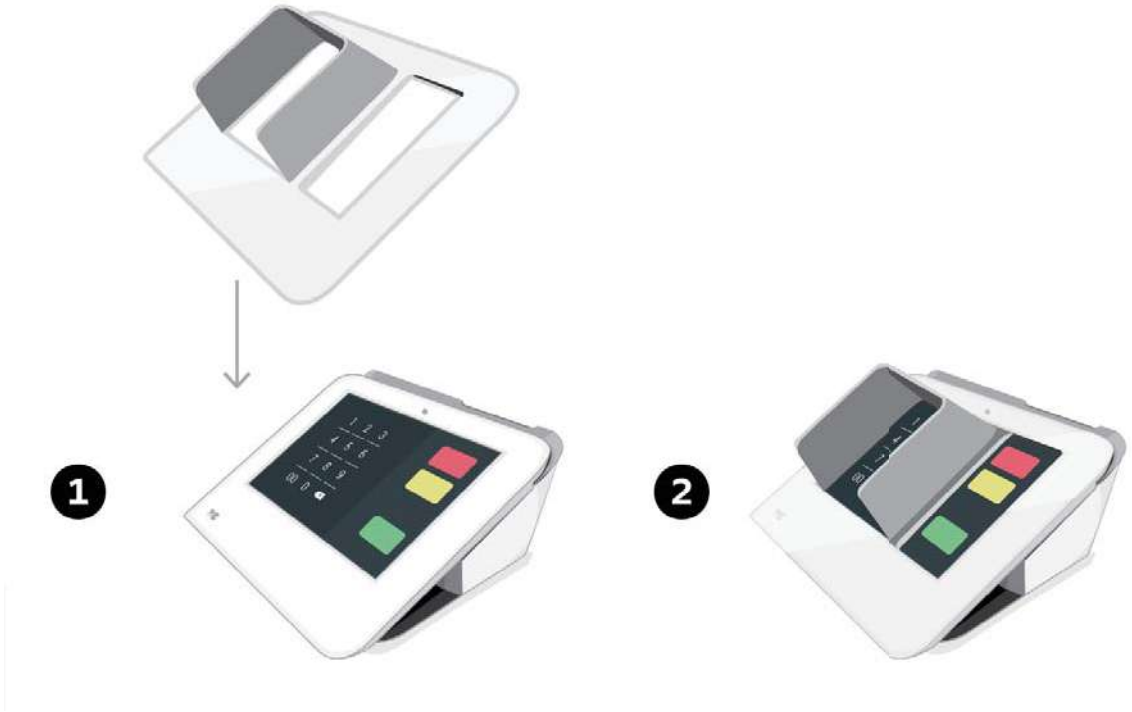
2. Software Development Guidance
    a. Clover Mobile software implements PCI security requirements for authenticated applications.
    b. No external developers are permitted to touch unencrypted payment data. Clover makes certain that this data is already encrypted immediately, that no clear-text data is outputted, and that all applications are signed.
    c. There are two types of APKs used for running software on the device:
        i. System Image APKs are controlled by the vendor. These APKs are signed with the Clover Platform App Validation Keypair. A hash of the each APK is also included in the system files list checked at boot. The app that controls payments is a System Image APK.
        ii. Data Image APKs are submitted by the developer and if approved by the vendor are signed by the source developer's key. Each APK has a whole file signature added and the APK is signed with the Clover App Validation Keypair. No data image APK has access to the payment systems.
    d. Non-Payment applications may install certificates into the system default keystore. Application developers developing non-payment applications should pin their server certificate (or public key) using one of the techniques described here: https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning
3. Networking the device
    a. If you are connecting the device via Wi-Fi, you must only connect to an access point that requires both username and password encrypted authentication.
4. Software update and patch procedures

a. When required, the device must install software updates. Updates are done over the air. If updates are not installed, the device will no longer be able to access the payment processing network.
b. The user is not required to do anything to receive the software updates.
c. Software updates cannot be performed via USB.

5. Self-tests are not initiated by the user. They include:
    a. Checking the integrity and authenticity of the software.
    b. Checking the security mechanisms for sign of tampering.
6. The following Open Protocols were considered during the PTS evaluation:
    a. Interfaces
        i. HSPA
        ii. USB
        iii. WiFi
        iv. Bluetooth [Disabled in Firmware and therefore excluded from PCI PTS Review]
    b. Protocols
        i. USB HID (keyboard & mouse), Serial, 3G modem driver, Ethernet
        ii. ICMP
        iii. TCP
        iv. UDP
        v. HTTPS (client)
        vi. DNS (client)
        vii. DHCP (client)
        viii. Bluetooth (L2CAP, ATT, AVCTP, AV Remote, AVDTP, Advanced Audio, AV Remote) [Disabled in Firmware and therefore excluded from PCI PTS Review]

## Visual Shielding

1. The device comes with a PIN Shield and supplied instructions on the proper installation and use. Use of the device for PIN Entry without the supplied PIN shield will invalidate the PCI PTS approval. The custom PIN Shield lays over the screen as follows:




2. In addition to the guidance on the PIN entry screen directing cardholders to shield their PIN entry with their hand, the merchant should take these additional precautions:
   A. Employees must be trained to provide verbal guidance instructing cardholders to shield their entry of a PIN number by covering the number pad with their hand.
   B. Any other customers who are "shoulder surfing" or standing too close to the cardholder must be directed far enough away from a cardholder to obstruct viewing during PIN entry.
   C. Surveillance cameras sited around the POS PED device must be positioned such that they cannot record the PIN number as it is entered.

## Device Security

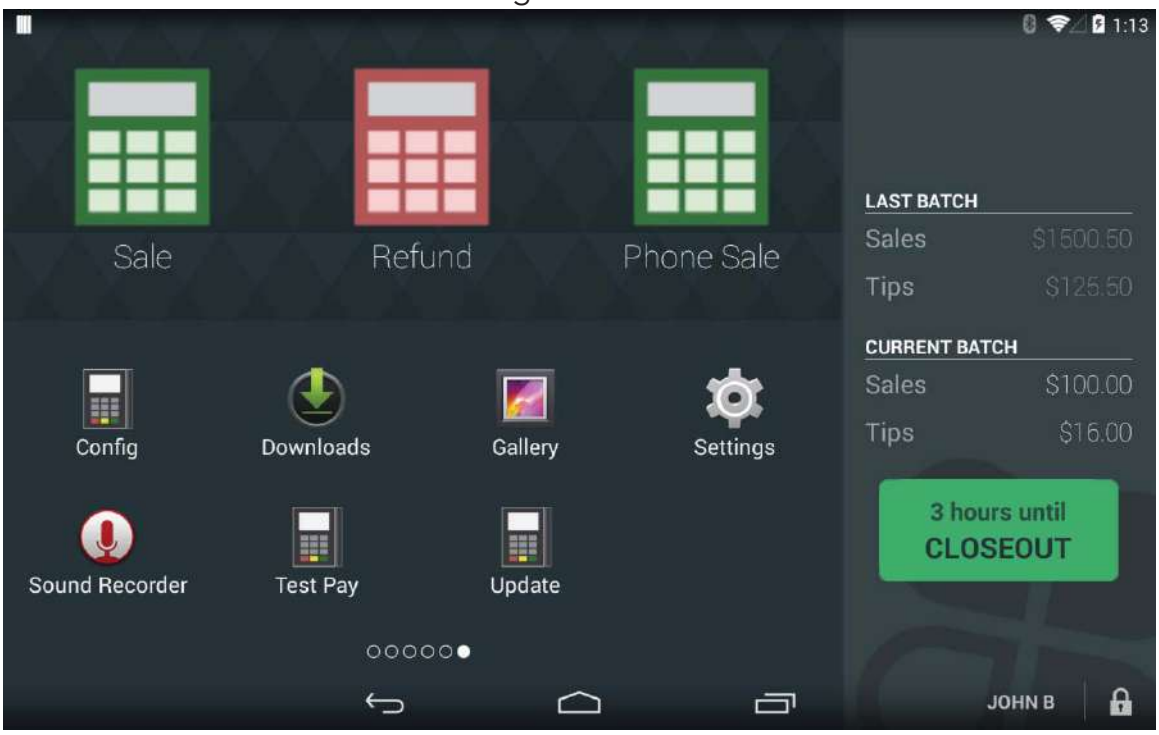
1. Roles

    a. 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.
2. Environmental Requirements
    a. The device should be operated under the following environmental parameters
        i. Maximum temp 135C
        ii. Minimum temp: -70C
        iii. Voltage ($V_{DD}$) high: 3.8V
        iv. Voltage ($V_{BAT}$) high: 3.8V
        v. Voltage ($V_{BAT}$) low: 2.1V
    b. Crossing these thresholds will trigger the tamper mechanisms. Tripping the tamper will require the device to be sent back to Clover.
3. Hardware Security
    a. The device contains a tamper mechanism.
    b. After a tamper event, all payment related keys are permanently erased. Payments will not be processed in this state.
    c. The device must be returned upon a tamper event and will not be reused.
4. Visual inspection
    a. Before using the device the user must conduct a regular inspection to check for evidence of tampering. The following is a partial list of procedures. Check the PCI website for the latest best practices.
        i. Exterior should show no evidence of cutting or disassembly
        ii. No evidence of unusual wires or overlays connected inside the ICC slot nor on or near the PIN entry area.
        iii. No changes to the resistance when inserting or removing a card from the ICC slot.

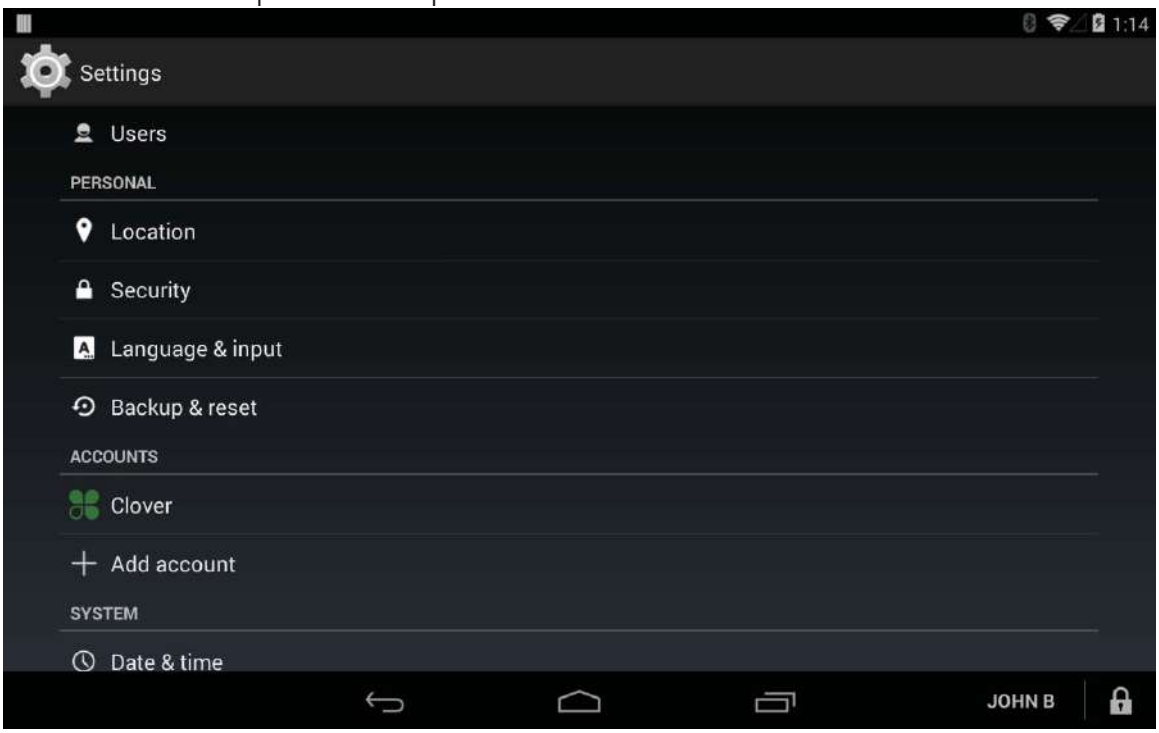
## Decommissioning

1. To decommission your device, a factory reset will remove the payment keys in the device. A device may then be provisioned to a new user.

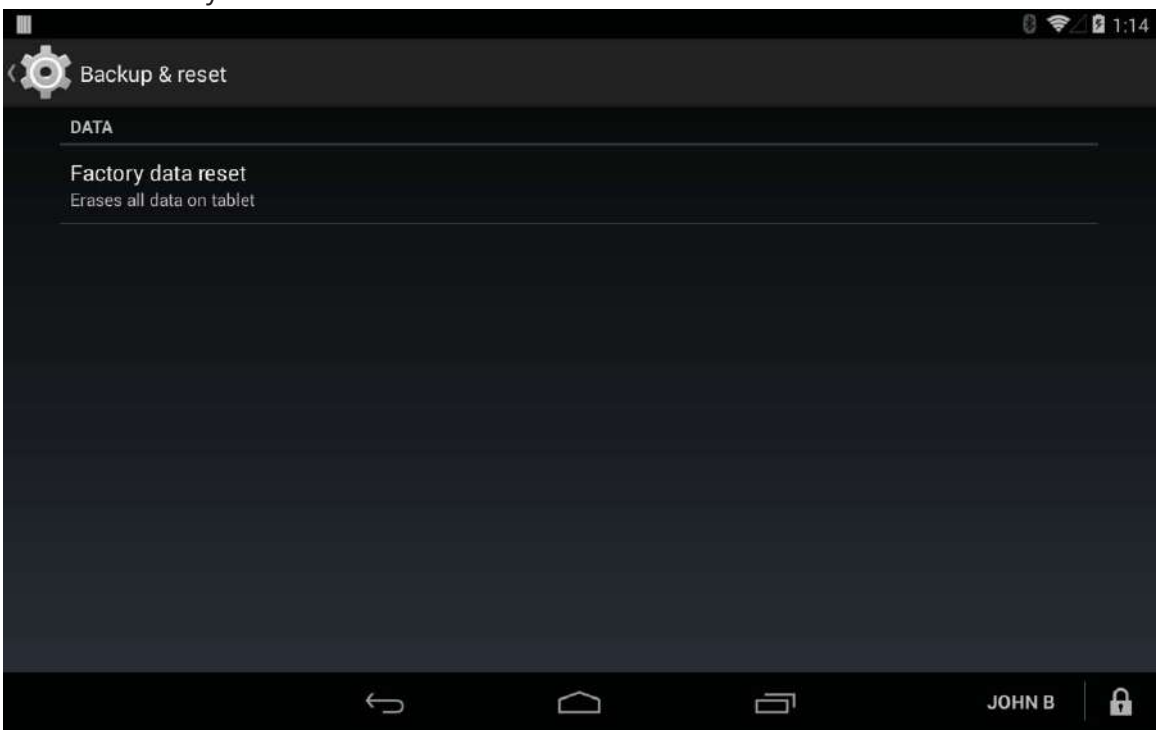
a. From the main screen select “Settings”:



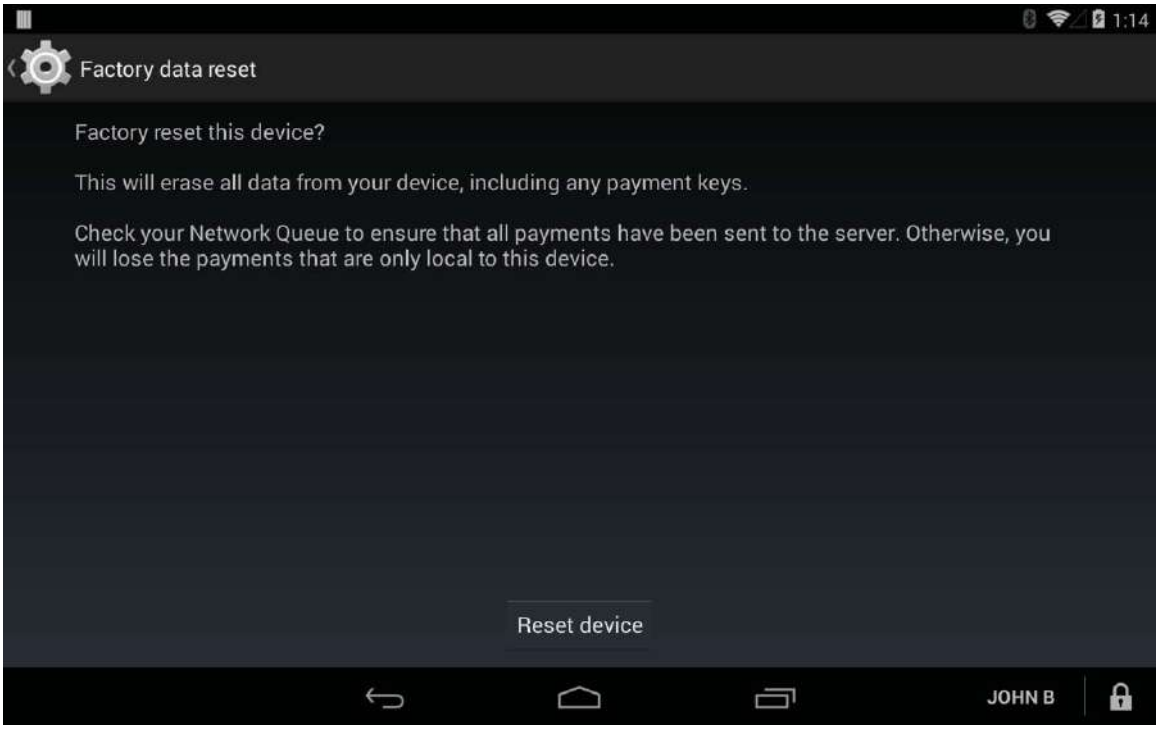

b. Select the “Backup & reset” option:



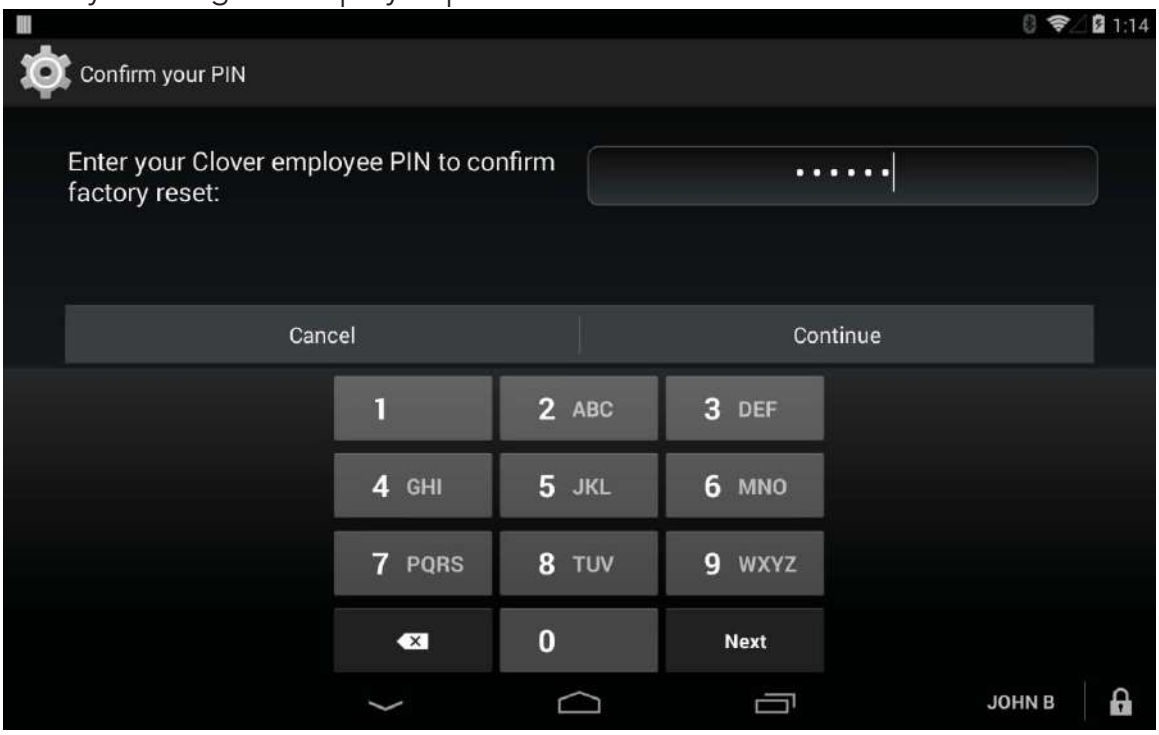
c. Select “Factory data reset”:



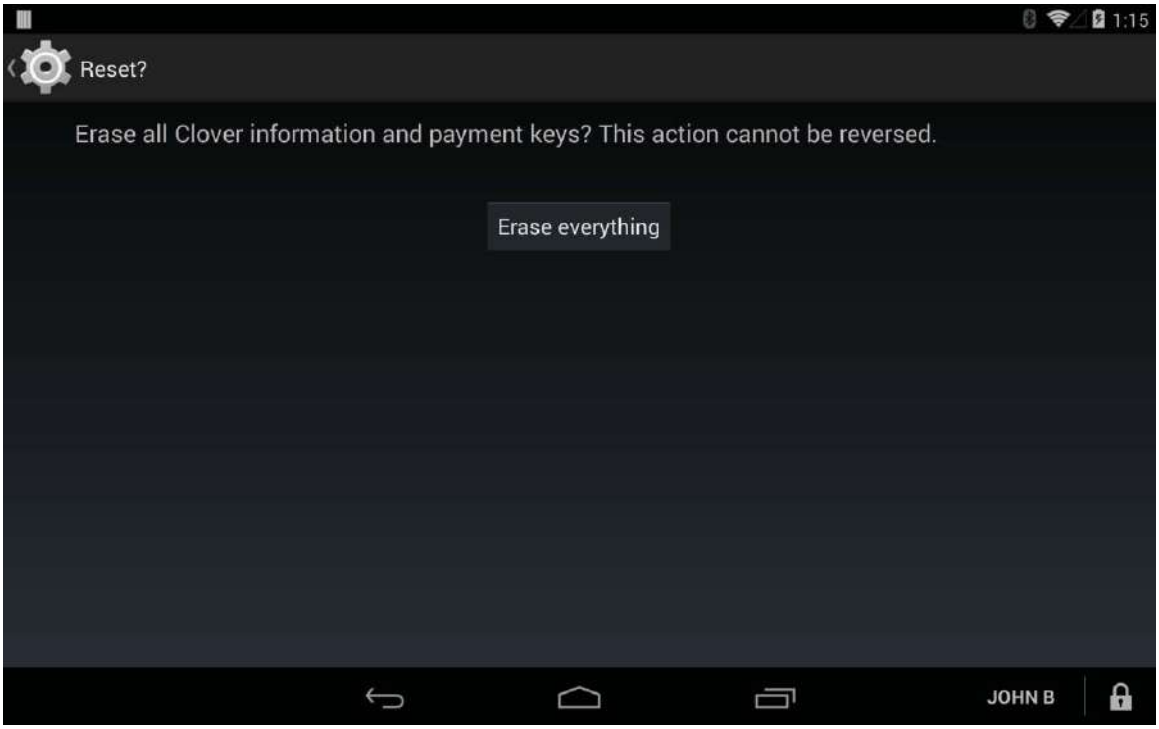

d. Select “Reset device”:



e. Enter your assigned employee pin:




f. Select “Erase everything”:



2. If a device's tamper mechanism has been tripped, the device's keys have been erased and the device needs to be returned to Clover.
3. If a device is damaged in any way that prevents the user from checking the commissioning status of the device, the device needs to be returned to Clover.
4. If the device needs to be disposed of by the user for any other reason, the device should be returned to Clover for decommissioning. Devices should not be disposed of by the user.

## Key Management

5. Key Management System
    a. The device uses a Remote Key Injection (RKI) process to distribute symmetric keys used to secure transactions. The keys are protected during distribution by a Public key Infrastructure (PKI) with X509 certificates.
    b. The process distributes 3 keys to terminals:
        i. PIN IPEK
        ii. SRED IPEK
        iii. MAC IPEK
    c. Although IPEK is an abbreviation for Initial Pin Encryption Key, it is used to refer to any initial symmetric key in a DUKPT key management system.
    d. The RKI process uses ANSI X9 TR-31 to distribute symmetric keys. Under TR-31, the key to be authenticated is both encrypted and authenticated via a symmetric Key Encryption Key (KEK).
    e. Before a device is delivered to a merchant, the device generates an RSA key pair. The public key is exported in a Certificate Signing Request (CSR). The CSR is then used to create an X509 certificate. The certificate is used to securely identify the device. The key generation and certificate issuance process is part of a PKI.
    f. When the merchant receives a device, it generates a RSA session key pair. The device then sends a RKI request to the Key Distribution Host (KDH). The RKI request consists of the public session key, the device metadata, the request's cryptological signature and the device's X509 certificate.
    g. When a device receives an RKI response, it first verifies the response signature. The device then uses the private session key

to decrypt the KEK. In turn, the KEK is used to extract the IPEKs from the TR31 containers. Once the IPEKs have been extracted, the RKI process is complete and the device is ready to process transactions.

h. There are no alternative key systems. The use of any alternative key management system would not work and would invalidate any PCI approval of this POI.

6. Cryptographic Algorithms
    a. All code is cryptologically authenticated before execution. The authentication process relies upon cryptological data stored in one time programmable memory (OTP memory). Once programmed, OTP memory cannot be rewritten so code signing keys cannot be replaced.
        i. Main Board (MB) - the mainboard uses 2048 bit RSA PSS to validate code. Main Board code is authenticated via the MB secure boot key (MB SBK). The bootloader cannot execute unless it is validated by the MB SBK.
        ii. Secure Board (SB) - the secure board uses 256 bit ECDSA to validate code. The secure board is protected by the Clover Root Key (CRK). The CRK is validated by the Maxim Root Key (MRK). At boot, the CRK is validated with the MRK. The CRK is then used to validate code.
7. Key Invalidation
    a. In the case of a compromise of a certificate authority operating by the vendor, the vendor will notify user and the device must be decommissioned according the instructions provided in that section of this document.
    b. In the case that you have been notified by the acquirer that the BDK or the IPEK has been compromised, you must decommission your device according the instructions provided in that section of this document.
8. Key table

| **Key Name** | **Purpose/Usage** | **Algorithm** | **Size** | **Stored** |
|---|---|---|---|---|
| Maxim Root Key (MRK) | Verify CRK | ECDSA | L=2048, N=256 (See FIPS 186-4 | Semiconductor Mask |

| | | | | |
|---|---|---|---|---|
| | | | Section 4.2) | |
| SB code signing key (CRK) | Verify SB ROM | ECDSA | L=2048, N=256 (See FIPS 186-4 Section 4.2) | Maxim 32550 OTP |
| SB Master AES Key | Encrypt data stored in crypto RAM | AES | 128 | Maxim 32550 hardware engine that encrypts crypto RAM |
| SB Auth Keypair | Identify and authenticate SB | RSA | 2048 | Private: NVS RAM; Public Key Certificate: MB |
| SB Enc Keypair | Used for encrypting messages sent to SB, in particular used to encrypt RKI TMK | RSA | 2048 | Private: NVS RAM; Public Key: SB |
| MB Auth Keypair | Identify and authenticate MB | RSA | 2048 | Private: MB (in msc partition encrypted under SSK); Public Key Certificate: MB |
| Device Root Keypair | Signs Device Intermediate Keypair | RSA | 2048 | MB ROM |
| PED Root Keypair | Signs PED Intermediate cert | RSA | 2048 | SB ROM |
| FD Manufacturer Root Keypair | Sign Manufacturer_Provisioning_CA | RSA | 2048 | SB ROM |
| RKI TMK | Symmetric key used to encrypt TR31 formatted IPEKs during remote key injection process | TDES | 112 | Maxim 32550 NVS RAM |
| KDH Root Keypair | Validating authenticitiy of remote key injection responses | RSA | 2048 | SB ROM |
| Clover KDH Signature Signer Keypair | Sign the RKI TMK Signature | RSA | 2048 | SB ROM |
| Transarmor Intermediate Cert Keypair | Validate authenticity of SRED RSA key (in case of RSA Transamor) | RSA | 2048 | SB ROM |
| TransArmor Keypair | Encrypt SRED data | RSA | 2048 | SB RAM |
| PIN IPEK | Initialize DUKPT key table | 3DES | 112 | Maxim 32550 NVS |

| | | | | |
|---|---|---|---|---|
| | | | | RAM |
| PIN DUKPT Future | Encrypt payment data. Used to derive DUKPT variants | 3DES | 112 | Maxim 32550 NVS RAM |
| SRED IPEK | Initialize DUKPT key table for SRED DUKPT Future | 3DES | 112 | Maxim 32550 NVS RAM |
| SRED DUKPT Future | Encrypt SRED data. Used to derive DUKPT variants | 3DES | 112 | Maxim 32550 NVS RAM |
| MAC IPEK | Initialize DUKPT key table | 3DES | 112 | Maxim 32550 NVS RAM |
| MAC DUKPT Future | Encrypt payment data. Used to derive DUKPT variants | 3DES | 112 | Maxim 32550 NVS RAM |
| Scheme CAPKs | Validate EMV card transactions | RSA | 2048 | MB linux filesystem; SB RAM |
| Merchant configuration signing keypair | Verify EMV parameters message sent to SB | RSA | 2048 | SB Code |
| Time Server Keypair | Verify time update message sent to SB | RSA | 2048 | SB Code |
| MB Secure Storage Key (SSK) | Protect data on MB (msc partition) | AES | 128 | Derived using SBK and dev key upon boot |
| MB SBK | SSK generation | AES | 128 | Tegra 4 efuse (unreadable) |
| MB Dev Key | SSK generation | IV for AES key derivation | 32 | Tegra 4 efuse (unreadable) |
| Flashing Server Keypair | Encrypting (MB SBK \| MB Dev Key) | RSA | 2048 | Public: MB TrusteZone |
| MB Bootloader PKC | Integrity protection of MB bootloader | RSA | 2048 | MB ROM |
| MB Kernel PKC | Integrity protection of MB kernel | RSA | 2048 | MB Bootloader |
| Debug block | Allows loading of signed debug blob | RSA | 2048 | MB ROM |
| Clover Developer Keypair | Validates authenticity of Clover-developed non-system apps | RSA | 2048 | MB ROM |
| Clover Platform App Validation Keypair | Authenticity of Android platform apps | RSA | 2048 | MB ROM |

| | | | | |
|---|---|---|---|---|
| Clover App Validation Keypair | Authenticity of non-platform Android apps | RSA | 2048 | MB ROM |
| Clover APK Validation Keypair | Authenticity of Clover Store Apps | RSA | 2048 | MB ROM |
| Clover Server Keypair | Identifies Clover's servers to device | RSA | 2048 | MB ROM |
| Clover Offline Keypair | Signs CAPKs, Revoked CAPKs and bin whitelist | RSA | 2048 | SB ROM |

## System Administration

There are no permissions granted to users regarding device security. The only action a user may take is to factory reset the device, which will erase all payment keys from the device and require it to be re-provisioned.