Clover Flex 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 5.0 document. This device is vendor-controlled. It is required that the vendor manage all payment security related functions.

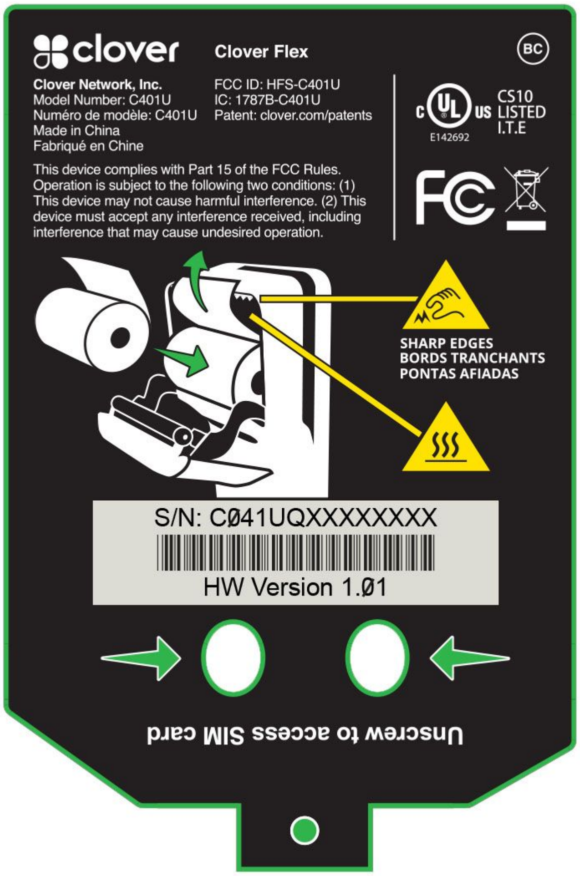
General description

1. Product overview
    a. Clover Flex is designed as a PIN entry device (PED) to facilitate credit- and debit-based transactions. 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.

2. Device Functionality
    a. This device obtains card data via Integrated Circuit Card Reader (ICCR), Magnetic Stripe Reader (MSR), manual card entry, 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 below



clover Clover Flex

BC

Clover Network, Inc.
Model Number: C401U
Numéro de modèle: C401U
Made in China
Fabriqué en Chine

FCC ID: HFS-C401U
IC: 1787B-C401U
Patent: clover.com/patents

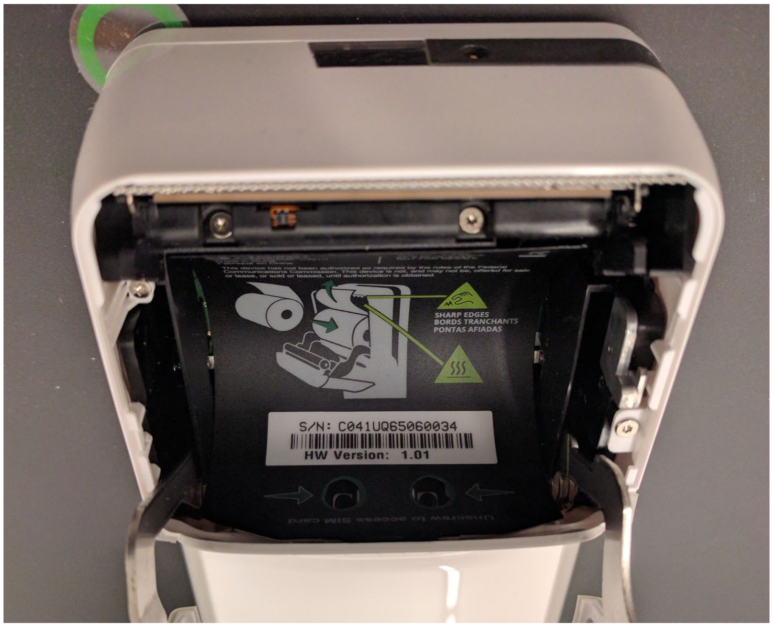
c UL us E142692 CS10 LISTED I.T.E

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference. (2) This device must accept any interference received, including interference that may cause undesired operation.

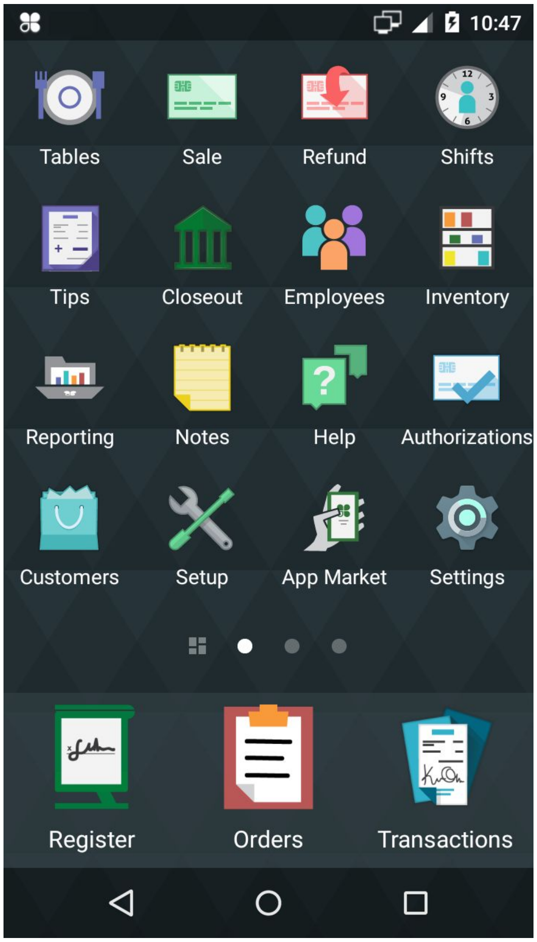
SHARP EDGES
BORDS TRANCHANTS
PONTAS AFIADAS

S/N: CØ41UQXXXXXXXX
HW Version 1.Ø1

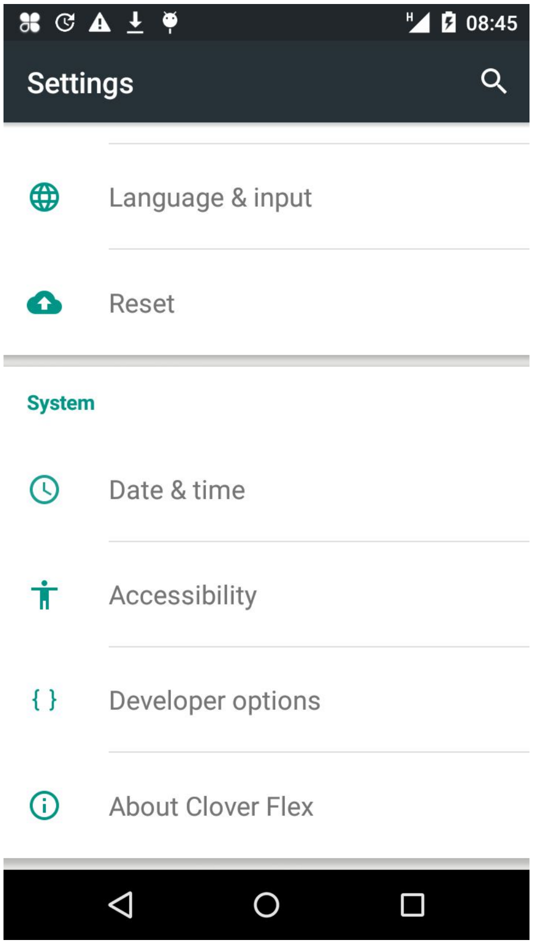
Unscrew to access SIM card



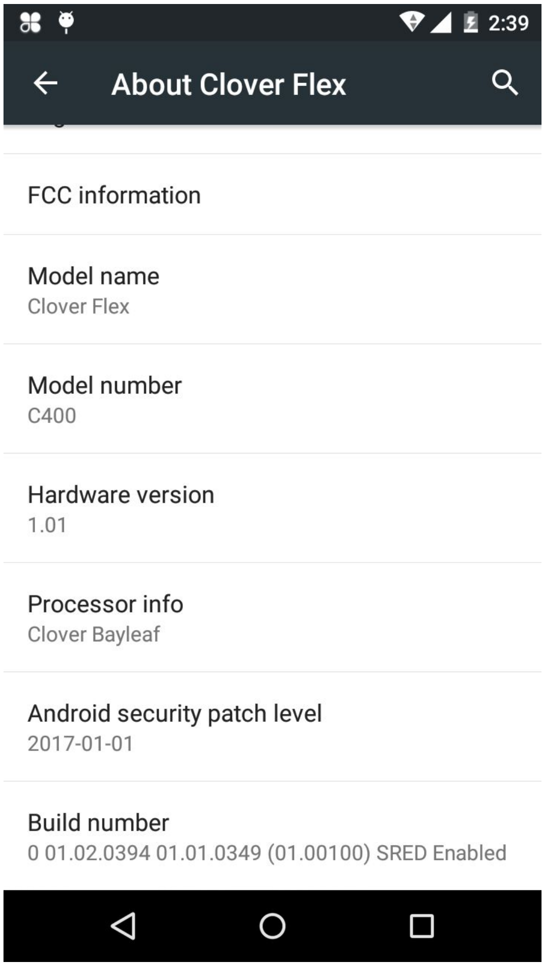
b. Version Information
c. Software and firmware are displayed on the Settings section on the device. The user should regularly check the software and firmware version of the device.
d. From the main screen, tap on “Settings”


10:47
Tables
Sale
Refund
Shifts
Tips
Closeout
Employees
Inventory
Reporting
Notes
Help
Authorizations
Customers
Setup
App Market
Settings
Register
Orders
Transactions

e. Tap “About Clover Flex”



f. View version numbers



About Clover Flex

FCC information

Model name
Clover Flex

Model number
C400

Hardware version
1.01

Processor info
Clover Bayleaf

Android security patch level
2017-01-01

Build number
0 01.02.0394 01.01.0349 (01.00100) SRED Enabled

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 inspect the device to validate the device' authenticity and integrity. To inspect the device, follow the instructions for daily inspections in the *Device Security* section below.
   c. After inspecting 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 secured at a level equal or greater than WPA or WPA2.

   d. 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. The device verifies the code by connecting to the server with cryptological authentication

   e. Once the code is verified against the requesting device, the device shall perform security updates including injection of security keys. The key injection process includes cryptological validation of the devices authenticity and integrity.

   f. If the code cannot be validated, it means that the secret information in the device does not match the information on file for the device and that the device cannot be used for PCI PTS payments.

   g. 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.

2. Software Development Guidance

   a. Clover Flex 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 the end user is connecting the device via Wi-Fi, she must only connect to an access point that requires both username and password encrypted authentication.
b. Any other Wi-Fi networking option will not work and would invalidate any PCI approval of this POI.

4. Software update and patch procedures
   a. When required, the device must install software updates. Updates are done over the air. Security critical updates are automatically installed without merchant intervention.
   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. Unattended Usage.
   a. Clover Flex is not designed for unattended usage as defined in PCI PTS. The use of the device in an unapproved method will violate the PCI PTS approval of the device.
7. The following Open Protocols were considered during the PTS evaluation:
   a. Interfaces
      i. HSPA
      ii. USB
      iii. Wi-Fi
      iv. Bluetooth
   b. Protocols
      i. USB HID (keyboard & mouse), Serial, 3G modem driver, Ethernet
      ii. ICMP
      iii. TCP
      iv. UDP
      v. HTTPS w/ TLS 1.2 (client)
      vi. DNS (client)
      vii. DHCP (client)
      viii. Bluetooth (L2CAP, ATT, AVCTP, AV Remote, AVDTP, Advanced Audio, AV Remote)
   c. Only TLS 1.2 is supported. SSL is not supported.
   d. Any other communications interface or protocols will not work and would invalidate any PCI approval of this POI.

Visual Shielding

1. Clover Flex is approved for handheld use.
   a. Any other use violates the device's PCI PTS approval.

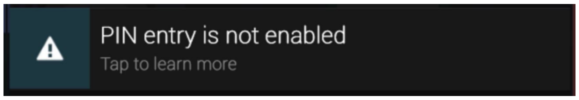
2. To deter visual observation of the PIN, the merchant should take these precautions:
    a. Train employees to provide verbal guidance instructing cardholders to shield their entry of a PIN number by covering the number pad with their hand.
    b. Ensure any other customers who are "shoulder surfing" or standing too close to the cardholder are directed far enough away from a cardholder to obstruct viewing during PIN entry.
    c. Position surveillance cameras sited around the POS PED device 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 operating temperature: 40° C
        ii. Minimum operating temperature: 0° C
        iii. Maximum storage temperature: 60° C
        iv. Minimum storage temperature: -20° C
        v. Minimum Secure Element Voltage: 2.0V
        vi. Maximum Secure Element Voltage 3.63V
        vii. The device is not designed to operate beyond these thresholds. If the device significantly exceeds these thresholds, the device's tamper mechanisms may be triggered. Triggering a tamper will require the device to be sent back to Clover to re-enable PCI PTS functionality.
3. Hardware Security
    a. The device contains a tamper mechanism.
    b. After a tamper event, all PCI PTS secret payment keys are permanently erased.
    c. A tampered device cannot be used to process payments in PCI PTS compliant manner.
4. Self Tests
    a. The device reboots and performs a self test every 24 hours.
        i. The reboot time is merchant-configurable. Any change to the reboot time will cause an additional reboot to ensure the device always reboots every 24 hours.
    b. The self test involves cryptologic validation of all code.
5. 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.

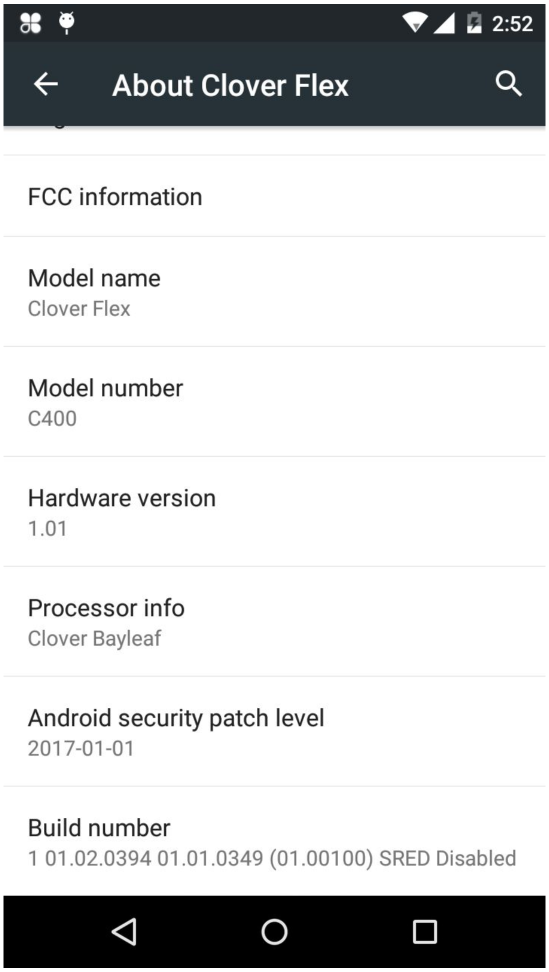
6. Tampered device
   a. When the device is tampered a notification will be displayed.



PIN entry is not enabled

Tap to learn more

7. A tampered device can be configured to temporarily accept MSR payments using an authenticated message sent from the Clover server. The version displayed by such a device will change to indicate disablement of SRED:



2:52

About Clover Flex

FCC information

Model name
Clover Flex

Model number
C400

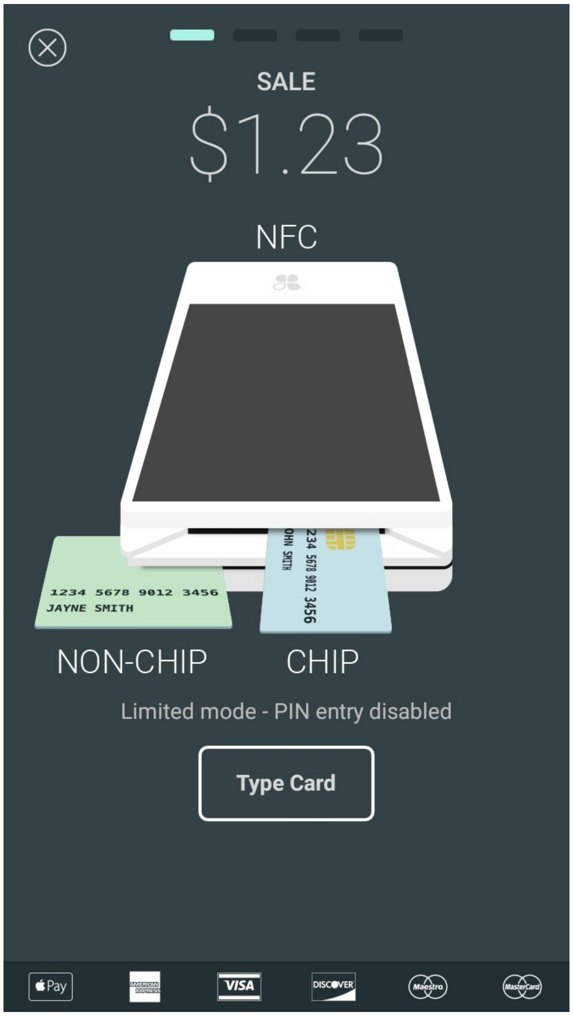
Hardware version
1.01

Processor info
Clover Bayleaf

Android security patch level
2017-01-01

Build number
1 01.02.0394 01.01.0349 (01.00100) SRED Disabled

a. Additionally, it will display the following alert when making payments:



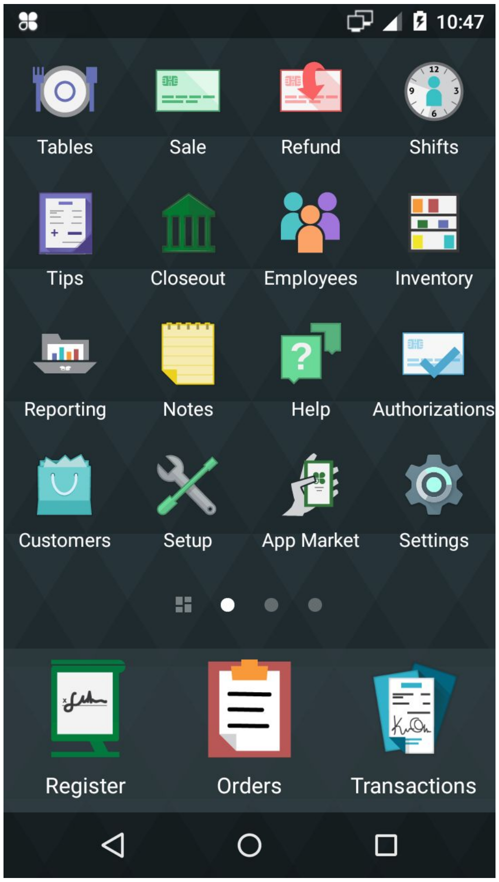
Limited mode - PIN entry disabled

8. The device uses BIN whitelisting with cryptographic authentication. The BIN whitelisting signing keys are managed by the vendor. The device does not support merchant-configurable SRED BIN whitelisting.

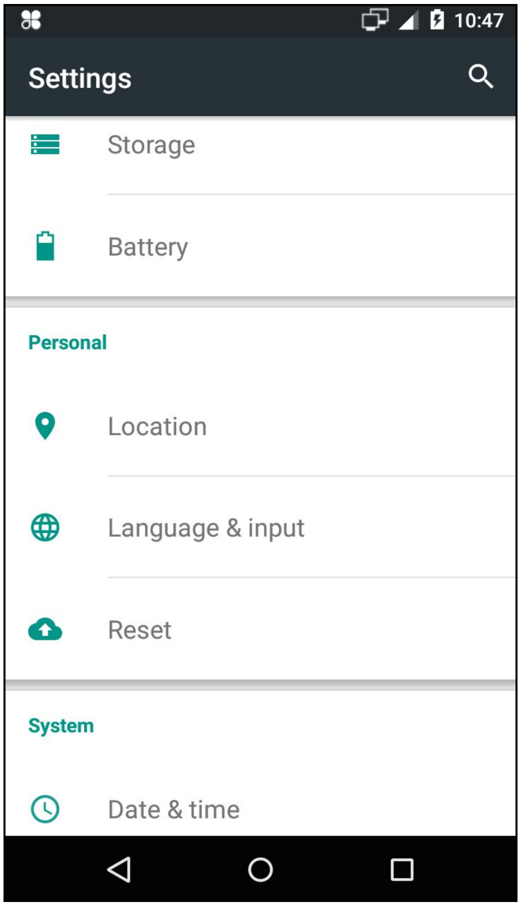
Decommissioning

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

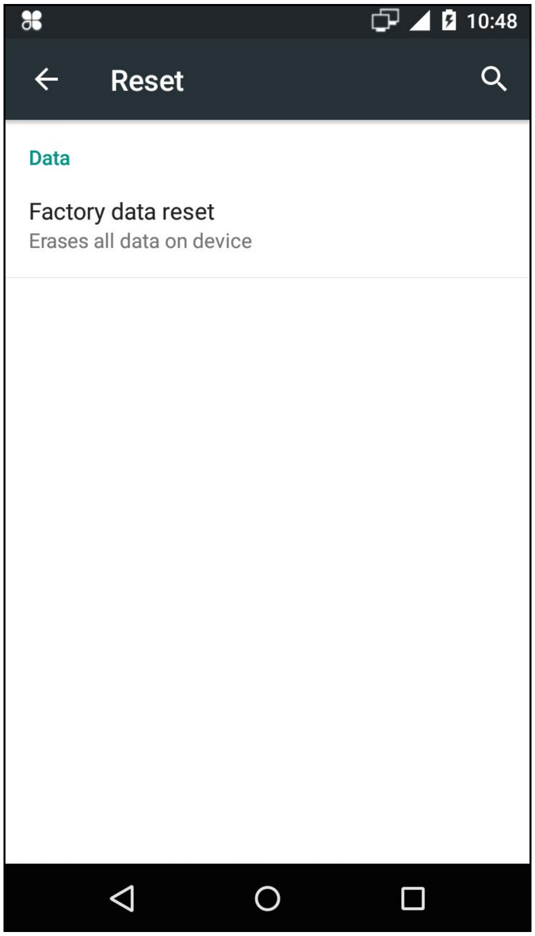
a. From the main screen select “Settings”:



b. Select the “Reset” option:



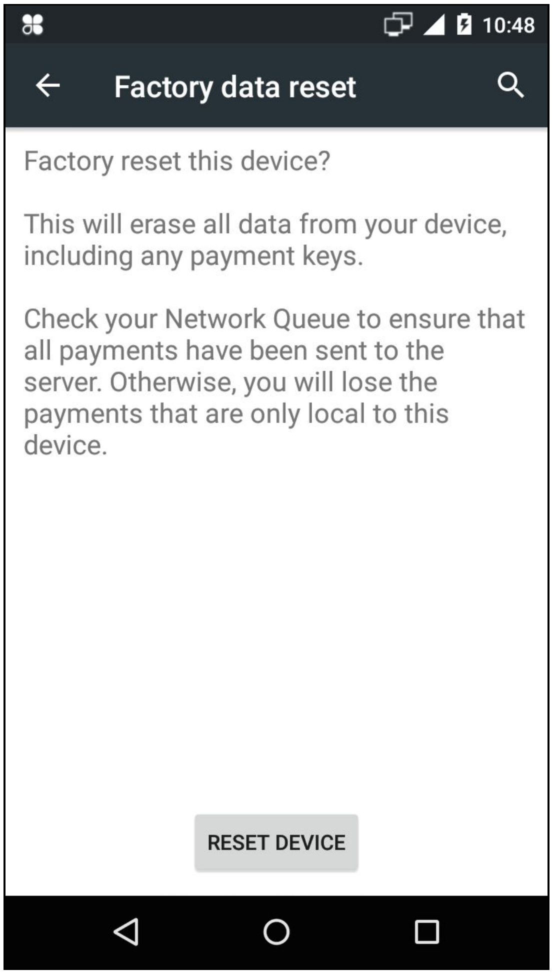
c. Select “Factory data reset”:



Data

Factory data reset
Erases all data on device

d. Select “Reset device”:

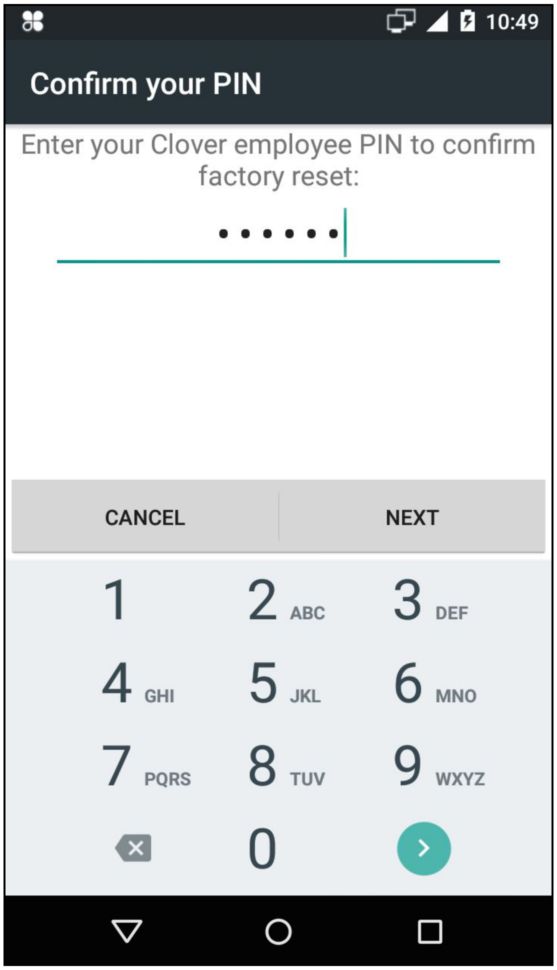


Factory reset this device?

This will erase all data from your device, including any payment keys.

Check your Network Queue to ensure that all payments have been sent to the server. Otherwise, you will lose the payments that are only local to this device.

e. Enter your assigned employee PIN:

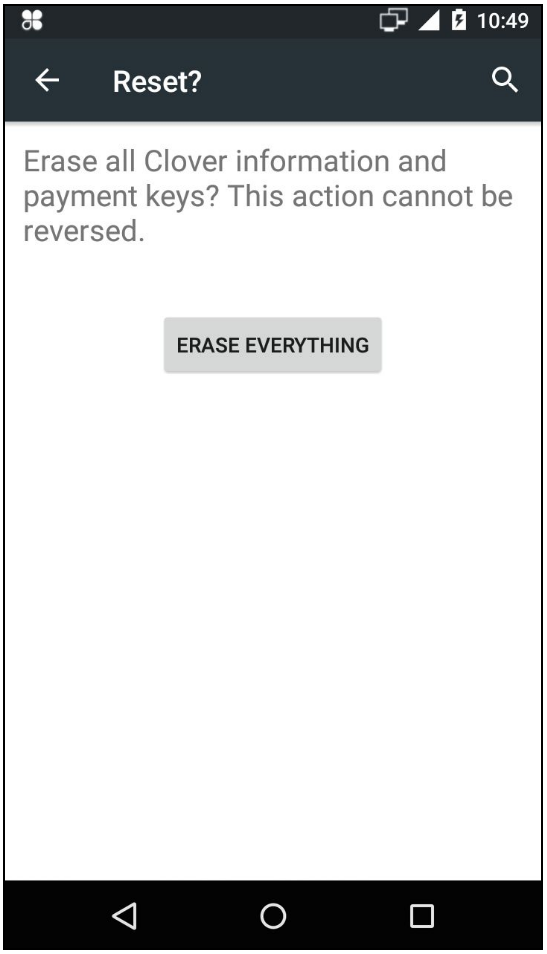


Confirm your PIN

Enter your Clover employee PIN to confirm factory reset:

••••••

f. Select “Erase everything”:



Erase all Clover information and payment keys? This action cannot be reversed.

2. If a device’s tamper mechanism has been tripped, the device’s keys have been erased and the device can no longer be used for PCI PTS compliant payments.
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 three 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 a 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 me rchant 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.
i. Account data is protected with either RSA-2048 (PKCS 1 OAEP w/ SHA256) or 3DES DUKPT. The account data protection settings are not merchant-configurable.

6. Code Authentication
    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. Application Processor (AP) - the AP uses 2048 bit RSA X509 Certificate hierarchy to validate code. The hash of the root certificate is burned into AP one-time programmable memory.
        ii. Secure Processor (SP) - The SP uses 2048 bit RSA X509 Certificate hierarchy to validate code. The hash of the root

certificate is burned into SP one time programmable memory. In addition, the SP firmware is validated at runtime with a HMAC key unique to each device.

7. Key Invalidation
   a. In the case of a compromise of a certificate authority operating by the vendor, the vendor will notify the user and the device must be decommissioned according the instructions provided in that section of this document.
   b. In the case that the end user has been notified by the acquirer that the BDK or the IPEK may have been compromised, she must decommission her device according to the instructions provided in that section of this document.
   c. This device should not be used after any keys become vulnerable to exhaustive brute force attack, as defined by NIST SP 800-57-1.

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.