



Reader for contactless and chip [SPC1-01]

Security Policy and Procedures

Table of Contents

- Version Control
- Introduction
- Installation and User Guidance
- Reader Authentication and Use
- Reader Security

Version Control

Version	Effective Date	Author(s)	Version Description
1.0	7/31/2018	Square Inc	Document Creation and Publication

Introduction

Square's POI SPC1-01 (Reader for contactless and chip) enables acceptance of EMV based transactions. It meets the security requirements published by the Payment Card Industry (PCI) Security Standards Council (SSC), PIN Transaction Security (PTS) Point of Interaction (POI) standard, version 5.1.

The purpose of this document is to inform Square sellers of how to use the Reader in a secure fashion, including information on key-management responsibilities, administrative responsibilities, device functionality, identification, and environmental requirements. The security policy defines the roles supported by the Reader and indicates the services available for each role. The POI is capable of performing only its designed functions—i.e., there is no hidden functionality. The only approved functions performed by the Reader are those allowed by the policy.

For a tutorial on how to get started using this device, [click here](#).

Installation and User Guidance

The Square Reader for contactless and chip (“Reader”) is a secure payment device that is designed for use by merchants in many industries for accepting card-present payment transactions. The Reader only works with the Square Point of Sale application and a compatible mobile device. There is no configuration of the Reader required other than to verify that the Reader is fully powered and connected via a USB port to the Square Stand or via bluetooth.

Initial Inspection

Upon receipt of the Reader, the Seller should inspect that the hardware version and serial number are visible on the underside of the Reader. The correct hardware version number for this approved reader is SPC1-01.

Bottom view:



Top view:



Front view:



Back view:



Installation

Before setting up your Square [Reader for Contactless and Chip](#), make sure you have a [compatible device with the latest version of the Square app](#).



For a full overview on setting up your reader, [watch this video](#).

1. Check the Battery of Your Square Reader

For an accurate battery reading, unplug your reader from any power source.

Firmly press and release the button on the reader. Green lights indicate that you're charged and ready to go. If you see a single red light, charge up immediately. Once your reader is on, you don't need to worry about turning it off. It'll automatically go into sleep mode after 2 hours of inactivity. To wake it up from sleep mode, firmly press the button on the side of the reader.

2. Charge Your Square Reader

Connect one end of the accompanying USB cable to your reader and the other end to a USB port like a cell phone charger, computer, or car charger.

It will take around 2 hours for a reader with low battery to charge completely.

3. Wirelessly Connect Your Square Reader

The new reader connects wirelessly with Bluetooth Low Energy (Bluetooth LE). Be sure you have the latest version of the Square app for your device—only the latest version supports the contactless and chip card reader .

Watch [this video](#) to learn how to wirelessly connect your reader

Connecting You'll need to connect through both your device's Bluetooth settings and through the Square app.

To connect your reader:

1. Press and release the button on your reader to turn it on.
2. Go to your device settings and make sure Bluetooth is turned on.
3. Open the Square app and tap: Three Horizontal Lines or the down arrow at the top of the Square Point of Sale: Register Switcher



4. Tap Settings > Card Readers > "Connect a Reader." On an iOS device, tap "Contactless + Chip Reader."



5. Put your reader into pairing mode by pressing the reader's button for 3-10 seconds.
6. Remove your finger as soon as you see orange flashing lights. If you see red flashing lights, you've held the button too long and you'll need to try again

When connected, the reader will be listed as Ready in-app.

Any necessary firmware updates will be automatically installed once the reader has been connected.

Note: The wireless connection can be lost if the reader and device are more than 10ft apart.

Reader Authentication and Use

Authentication of the Reader

Upon receipt, the Seller can connect the Reader to the USB hub of the Square Stand or to their mobile device using bluetooth. The Reader is cryptographically authenticated to both the Point of Sale application and the Square back-end servers. If the Reader is valid, it will register as such with the Square Point of Sale application. If the Seller has received an unauthorized reader, the Square Point of Sale application will indicate that the reader cannot be used with the application. The Seller does not have permissions to configure the Point of Sale application or Reader settings for the authentication function.

Using the Reader

How to obtain a Reader

The Reader may be obtained either via the Square website www.squareup.com or via an approved retail location. The Reader is ready for use upon receipt. The Seller should verify that Square offers payment processing in their country of intended operation, from a retailer located in the same country.

Attributes of a Reader

The Reader has the following approval classes: Secure Card Reader - PIN. The Reader is intended for use in environments with attended and semi-attended payments; it is not intended for use as an unattended payment terminal (UPT). Use of the device in an unapproved method invalidates the PCI PTS approval of this device.

How to store a Reader

To store the Reader simply remove it from the Square Stand USB port and store for next use. In the event the Seller will not use the Reader for more than twelve (12) months at a time, be sure to charge the Reader prior to storage and periodically to preserve its readiness. If the Reader is not fully charged annually it will enter into a tampered state and become inoperable.

Procedures for using a Reader

It is important that each day or before use the Seller check the Reader to make sure it has not been tampered with between uses. This can be easily done by looking at the chip card slot to verify there are no foreign objects such as capture devices, card skimmers, extra wires/cables or other materials.

The Square Point of Sale application will convey operational messages from the Reader including when the device is ready for payment and when a payment data capture is complete. The Reader has no user-configurable security options.

Security Self-Tests

In addition to the continual tamper detection and response, the Reader authenticates the firmware and terminal configurations using RSA 3072/SHA-256 every time it is powered on. The Reader also implements a forced reboot every 23.5 hours which initiates the same self-tests as when the device is powered on.

How to decommission a Reader

To decommission the Reader please ship the device to the following address for decommissioning:

Square, Inc.
c/o : Reader Decommissioning
1455 Market St, Suite 600
San Francisco, CA 942103
USA

How to review the hardware and firmware version

A Square Seller can confirm the hardware version by physical inspection as described above. In addition, the Seller can confirm the hardware and firmware version via the *Settings > Card Readers* screen of the Square Point of Sale application.

The PCI approved firmware version is displayed as “SCRP.1.x.xx.xx”.

Reader Security

Privacy shielding

The Reader is not a PIN-entry device and has no screen or PIN pad available to disclose information.

Firmware and software update

Square will update the firmware associated with the Reader automatically as needed. This will occur automatically with limited Seller interaction required. In the event of a critical update, the Square Point of Sale software will notify the Seller of the critical nature of the update and advise a course of action for applying the update. Based on the criticality of the update, Square may disable transaction processing until a firmware update is successfully applied.

Infrequent or seasonal use

The Reader has a primary battery and backup battery. The primary battery is used for operation of the Reader. The backup battery is used to maintain the tamper-detection features of the Reader. If the primary battery is entirely discharged the backup battery will maintain tamper-detection of the device for one year. If the Reader is not fully charged annually it will enter into a tampered state and become inoperable.

Common use and recharging of the primary battery will prevent the Reader from entering a tampered state. For infrequent or seasonal users of the Reader we recommend charging the Reader fully at least once each year.

Tamper detection and response

External Inspection of Reader

Under normal operation, the Reader employs internal active tamper-response mechanisms as described below. These mechanisms are enforced automatically and do not require any initial configuration by the user.

Prior to accepting payments with Reader, the user must inspect the Reader for evidence of external tampering. Procedures should include, at minimum, examination to identify:

- Evidence of inserts, wires, overlays or any unknown component connected to the Reader or inside the card slot
- Evidence of modification or disassembly of the Reader
- Visible or tactile changes to the cable connections or card slot

Please contact [Square Support](#) if you discover any evidence of external tampering.

Automatic Tamper Response

The Reader may identify certain events as attempts to tamper with its operations to alter its inner workings. If the Reader identifies a tamper event it will erase the encryption key material it contains and become inoperable.

The Reader is rated for normal operation and any of the below scenarios may tamper the device and cause it to become inoperable:

- Temperatures outside of the range of 0 and 40 degrees Celsius
- Voltage greater or less than 5V input for charging the device via USB
- Any attempt to open/disassemble/take apart the Reader or access parts inside

The Reader is intended to be fully charged once a year. If the Reader's primary battery is fully discharged and left for more a year without a recharge it may become inoperable.

The Seller can detect if a tamper event has occurred by connecting the Reader to an approved mobile device with the Point of Sale application installed. Opening the Point of Sale application will notify the Seller if the device has reached a tamper event.

If the Reader experiences one of the above tamper events, Square will reach out to the Seller and communicate as appropriate how to return the Reader to Square for secure disposal and replacement.

Software Development Guidance

The Reader is designed for use with Square products and applications, and does not work with other applications. All code is developed, written, and managed by Square. Square developers must refer to the Software Engineering and Vulnerability Management Procedures when developing new software for Readers.

Encryption and key management

The Reader is only intended for use with other Square applications and services. Square performs all key management, key loading, and acquiring. Attempts to operate the device with any other key loading, acquirer, or key management will render the device inoperable. In addition, the use of the device with different key management systems will invalidate the PCI approval of this device.

All of the cryptographic keys used by the Reader to protect the confidentiality and integrity of sensitive data are injected at the time of manufacture using a Square-proprietary protocol. The keys are stored within the Reader's secure boundary, and are protected from

both disclosure and modification; such protection is achieved with a key-encrypting key that meets the PCI PTS key strength requirements. Sensitive data is encrypted by a unique key per transaction using AES CCM, which is an authenticated encryption mode for AES that provides both confidentiality and authentication.

The Reader only supports injection of keys during the manufacturing process; no remote key injection is required as the Reader communicates directly with Square servers. During the manufacturing process, Square's key provisioning equipment authenticates incoming readers. Readers entering the key provisioning stage authenticate the key-bundles received as having originated from Square's factory key provisioning module. The Reader does not accept keys from any entity other than the factory provisioning module. Using the Square-proprietary protocol, the cryptographic keys are injected into new devices in encrypted form. The Square keys are injected and maintained under Square control and the details are transparent to the merchant.

The Reader does not provide or allow any user-configurable encryption key management functions.

Thank you for reading!