SumUp air

SECURITY POLICY

SumUp air Security Policy
December 20, 2016

Comments? Please e-mail all comments in this document to your local SumUp Support Team.

SumUp Payments Limited

www.sumup.com

SumUp [air] Security Policy

Contents

Document Overview

This document addresses the proper use of SumUp air in a secure manner including information about key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements.

Failure to use of the device in accordance with this security policy will violate its PCI PTS 4.x compliance and approval.

Audience

This guide provides simple descriptions of SumUp [air] features, as well as basic information for anyone installing and configuring SumUp [air].

Acronyms

AES	Advanced Encryption Standard
DUKPT	Derived Unique Key per Transaction
N/A	Not Applicable
PED	PIN Entry Device
PIN	Personal Identification Number
RSA	Rivest Shamir Adelman Algorithm
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard

References and Related Documentation

[1] SUMUP AIR User Manual
[2] SUMUP AIR Firmware API Specifications
[3] SUMUP AIR Software Design Specifications
[4] SUMUP AIR Application Development Guidelines
[5] ANS X9.24-1:2009, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques
[6] ANS X9.24 Part 2: 2006, Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques for the Distribution of Symmetric Keys
[7] X9 TR-31 2010, Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms
[8] ISO 9564-1, Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems
[9] ISO 9564-2, Banking — Personal Identification Number management and security Part 2: Approved algorithms for PIN encipherment
[10] PCI PTS POI Derived Test Requirements V4.0 - June 2013
[11] RSASSA-PKCS1-V1_5 (RSA sign/verify) defined in PKCS#1 v2.1 Draft 2 January 5, 2001)
[12] Integrated Circuit Card Specification for Payment System, Book 2 Security & Key Management, Version 4.3, November, 2011

Note: [1] is delivered to the end-user, [2,3,4] are delivered to authorized application developers

Product Description

The SumUp air unit is a handheld PIN pad with an integrated smart, magnetic stripe, and contactless card reader, offering advanced security and payment processing capabilities to handle credit and PIN-based debit card transactions in an attended environment.

SumUp air supports both symmetric encryption algorithms (DES, 3DES, and AES) and asymmetric encryption (RSA). This device internally manages simultaneous multiple keys through either Fixed, Master Session- or DUKPT-based processes, and offers high performance smart card processing, as well as support for the new generation of 3-volt cards. The SumUp air sleek and stylish ergonomic design offers power and performance in a smart, MSR, and contactless-integrated PIN pad device.

Features and Benefits

Exceptional Ease of Use

• Ergonomic design is sleek, stylish, and lightweight for conveniently handing the unit to the consumer for PIN entry.
• Intuitive interface and large, colored control keys simplify training and reduce support requests.
• Highly readable display handles multiple languages.

Critical Security Protection

• Incorporates tamper-detection circuitry to resist unauthorized intrusion and supports a broad spectrum of hardware and software-based security features.
• Integrated security modules simultaneously support sophisticated encryption (AES, DES, 3DES, RSA) and key management schemes, including single and 3DES Master Session, single, and 3DES Derived DUKPT.

Strong Feature Set

The SumUp air PED is designed to handle all forms of payment including:

- EMV chip & PIN,
- Chip & Sign
- Magstripe
- Contactless

SumUp air provides an USB and Bluetooth connectivity options.

Product Identification

Product Name

The product name is printed on a label at the back of the device.

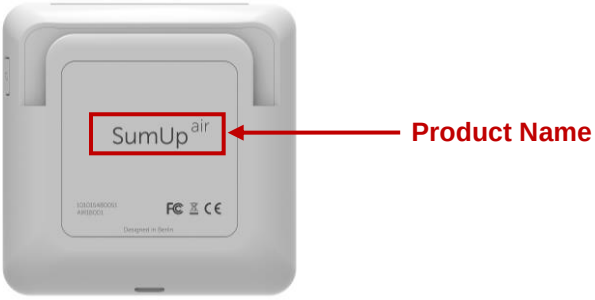

Figure 1 – Product Name Identification

Hardware Version

The product hardware version is printed on a label at the back of the device. The label at the back of the device shall not be teared off, covered or altered.

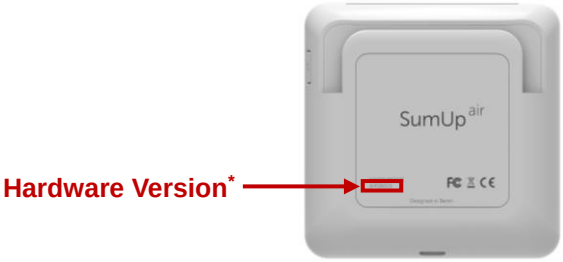

Figure 2 – Product Hardware Version Identification

Software Versions

The product firmware and/or application versions can be retrieved using a software menu on the terminal. To get this information press the ← button and select INFO VERSION:

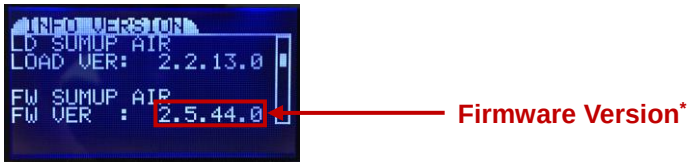

Figure 3 – Product Software Version Identification

*** Only the first two digits of the hardware and firmware versions are the PCI approved versions. The last two digits of the version indicate minor non-security related changes.**

Product Identification for devices with Bluetooth Low Energy 4.2

Product Name

The product name is printed on a label at the back of the device.

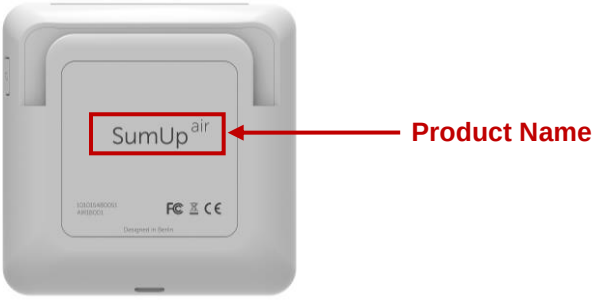

Figure 4 – Product Name Identification

Hardware Version "AIR1Exxx"

The product hardware version is printed on a label at the back of the device. The label at the back of the device shall not be teared off, covered or altered.

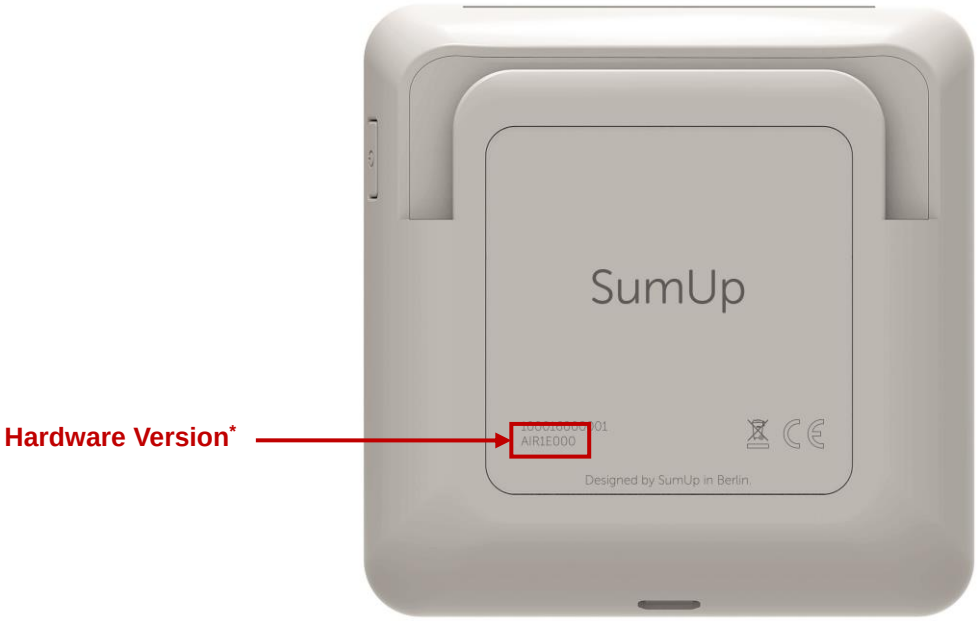

Figure 5 – Product Hardware Version Identification

Software Versions

The product firmware and/or application versions can be retrieved using a software menu on the terminal. To get this information press the button and select INFO VERSION:

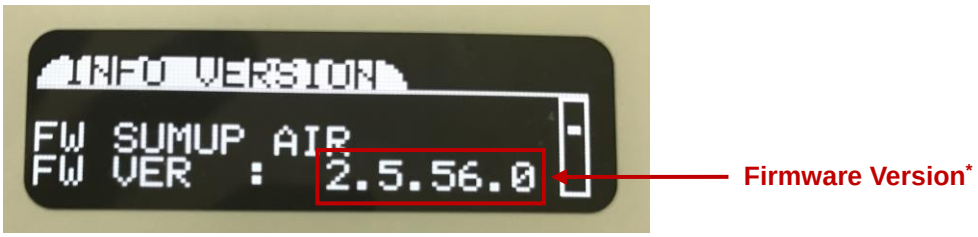

Figure 6 – Product Software Version Identification

*** Only the first two digits of the hardware and firmware versions are the PCI approved versions. The last two digits of the version indicate minor non-security related changes.**

Hardware Security

Initial Security Inspection

Upon receiving the SumUp air terminal, the merchant or acquirer must validate the shipment origin and sender name of the terminal to be genuine by verifying the courier tracking number and sender information located on the product order paperwork/invoice.

The terminal must be visually inspected for signs of tampering prior to placement in the field to ensure that the device has not been tampered with and is in original pristine condition.

Note: A User Manual[1] including the following information is provided with the device:

- Equipment check list:
  - Device,
  - Cable and connectors,
  - Documents
- Power and cable connections information,
- The main characteristics of the device (i.e. Temperature, humidity, voltage)
- Safety recommendations,
- Security recommendations,
- Troubleshooting if the device does not work.

SumUp air must be verified to be approved by PCI SSC as a PED (PIN Entry Device) on the official PCI PTS SSC portal:

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

- Locate the Product Identification Label(Figure 1 and 2) on the bottom of the device and verify that the product name and hardware version number match the product name and hardware version number shown on the PCI PTS listing web site.
- Compare the first two digits of the Firmware version (Figure 3) with the one listed in the PCI PTS listing web site.

Periodic Inspection and Maintenance

The following inspections must be performed on a regular basis after initial receipt and installation of SumUp air:

- There are no unusual wires connected to the ICC acceptor, the magnetic stripe slot, or any of the ports on the terminal.
- There is no shim device in the ICC acceptor slot.
- The keypad is firmly in place.
- No warning and/or flashing message is displayed on the screen.
- The terminal serial number(on the label) corresponds to the one in the inventory paperwork.

Note: Such checks would provide warning of any unauthorized modification to the terminal, or suspicious behavior of the terminal or suspicious behavior of individuals that have access to the terminal. In the tampered state, the device displays a warning message **[INVALID BPK!]** and further use of the device is not possible. If such a message is observed, the merchant or acquirer must contact the terminal helpdesk immediately, remove it from service and keep it available for potential forensics investigation. The merchant or acquirer should also check that the periodic inspections and maintenance are performed by a trusted person and log the periodic checks and maintenance operations, including name of the operator.

Terminal Service Removal

Sensitive data must be erased before refurbishing the terminal or removing it permanently from service. The terminal shall go to tampered status, a state in which sensitive data are erased. Note: Disassembly of the device will lead to a tampered status.

Terminal Environment Conditions and Environmental Failure Protection

The specified environmental conditions to operate and store the device are:

Operating: -10ºC to +45ºC / 5% to 90% RH
Storage: -15ºC to +55ºC / 5% to 90% RH

The security of the terminal is not compromised by altering the environmental conditions (e.g. subjecting the device to temperature or operating voltages outside the stated operating ranges does not alter the security).

Tamper Response Event

The device contains tamper mechanisms that will trigger when a physical penetration attempt of the device is detected. A merchant or acquirer can easily detect a tampered terminal:

- The Payment Application is not started,
- The numerical keyboard is not functioning,
- A warning message **[INVALID BPK!]*** is displayed.

*After FW version FW2.4.56.0 message is “**Device blocked. Please contact Support**”

Figure 7

Any physical penetration will result in a “tamper event”. This event causes the activation of tamper mechanisms that make the device inoperable out of service.

If the device is in tampered state, the merchant or acquirer should contact the terminal's helpdesk immediately, remove it from service and keep it available for potential forensics investigation.

Software Security

Software Development Guidance

When developing IP enabled applications, the developer must abide by the coding rules and best practices described in the SUMUP AIR Application Development Guidelines [4] document. The security guidance in the SUMUP AIR Application Development Guidelines [4] document describes how protocols and services must be used/configured for each interface that is available on the platform.
When developing SRED applications, the developer must follow the guidance described in the SUMUP AIR Application Development Guidelines[4] document for procedural controls to ensure that the applications are properly reviewed, tested and authorized.

The document provides security guidance for account data management and remote connection authentication using cryptographic mechanisms.

Firmware and Application Update

Updates to the firmware and the application can be loaded in the device. They are cryptographically authenticated by the terminal. If the authenticity is not confirmed, the update is rejected. For secure operation of the device, it is recommended to always use the latest version of firmware distributed.

Application Authentication

Application code is authenticated before being allowed to run. The signature of the application code is verified. In case of incorrect signature, the update is rejected. No action is expected from the end user. The signature is based on the RSASSA-PKCS1-V1_5 SHA-256 algorithm and 2048 bit keys. The authenticity is guaranteed by the manufacturer.

PIN Confidentiality

The intended use of SumUp [air] is as a handheld device in attended environment.
The PED will be given to the customer to enter the PIN. The body of the customer and the orientation of the PED towards him will protect the PIN entered from visual observation.

Self-Tests

Self-tests are performed upon start up/reset and also periodically – i.e. once a day and/or before every PIN entry. These tests are not initiated by an operator.
Self-tests include:
• Check of integrity and authenticity of the firmware, application and cryptographic keys

• Check of the security mechanisms for sign of tampering

Key Management

Key Loading Methods

There are 50 3DES and 8 DUKPT key slots available in the secure firmware of the terminal.

There are two key loading methods:

• TR-31 Key Derivation Method

• Custom Method – using Key Encryption Keys

Key Usage

• Encrypt/Decrypt Data

• MAC Calculation and Verification

• PIN Encryption

PIN Encryption Techniques

PINs are encrypted using an algorithm and key size specified in ISO 9564.

The algorithm for online PIN is the TDEA using the electronic code book (TECB) mode of operation as described in ANSI X9.65.

The device implements three different PIN encryption key-management methods:

Fixed Key, Master Key/ Session Key, DUKPT, as specified in ANSI X9.24

ISO 9564-1 PIN block formats 0, 1, or 3. Format 2 is used for offline PIN

Note: The use of the device with different key management systems will invalidate any PCI approval of this device.

Cryptographic Algorithms

The device supports the following algorithms:

3DES, AES, RSA, SHA

Key Table

KEY NAME	USAGE	ALGORITHM	SIZE	NUMBER OF AVAILABLE SLOTS
USER KEY	Random key for application data storage	AES	128	1
KEKTR31	Key Loading Key (TR-31 Method)	3DES	112	50*
KEKCUSTOM	Key Loading Key (Custom method)	3DES		
KEYPIN	Key used for PIN Encryption (Fixed, MK/SK)	3DES	112	50*
KEYMAC	Keys for ISO 9797-1 / ISO 16609 MAC calculation and verification.	3DES	112	50*
KEYENC	Key for Data Encryption	3DES	112	50*
KEYDEC	Key for Data Decryption	3DES	112	50*
KEYDUKPT	Key used for PIN, DATA, MAC	3DES	112	8
KEYCA	CA Public Keys	RSA	?	100

*Total number of slots available for all 3DES type keys

Key Replacement

Key replacement must be performed upon any known or suspected compromise of any cryptographic or sensitive information. Any key should be replaced with a new key whenever the compromise of the original key is known or suspected, and whenever the time deemed feasible to determine the key by exhaustive attack elapses.

Terminal Administration

Configuration Settings

The device is functional when received by the merchant or acquirer. No security sensitive configuration settings are necessary to be tuned by the end user to meet security requirements.

Default Value Update

The device is fully functional when received by the merchant or acquirer and there is no security sensitive default value that needs to be changed before operating the device.

Roles and Services

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.