

Strong Customer Authentication for Apple Pay on Mac mini with M2 and Magic keyboard with Touch ID, running macOS Ventura 13.3.1

Guidance

Version 1.4

October 17, 2023

Table of Contents

1. Introduction	3
2. Preparation Guidance	4
3. Identification	4
4. Operational Guidance	5
4.1. Configure Password	5
4.2. Check warranty status	6
4.3. Configure Touch ID	6
4.4. Update macOS	6
4.5. Apple Pay	6
4.6. Operational failures	6
4.7. Security Settings	6
4.8. Security updates, announces and registering	6
4.9. Trusted Root Users	6
4.10. Erase all content and settings – Disk erase	7
Annex A – Issuer Security Objectives	8
Annex B – Apple Server Security Objectives	9

1. Introduction

This document contains references to other documents providing guidance for security related topics specified in the Security Target.

Reference	Description
[AP]	Apple Pay Support https://support.apple.com/apple-pay
[APS]	Apple Platform Security, May 2022 https://support.apple.com/guide/security/welcome/web
[CHECK-SERIAL]	Check Your Service and Support Coverage (review your Apple warranty status) https://checkcoverage.apple.com
[ENROLLAP]	Set up Apple Pay https://support.apple.com/en-us/HT204506
[INITCFG]	Set up your Mac mini https://support.apple.com/guide/mac-mini/set-up-your-mac-apd831707cb3/mac
[MACRESET]	Erase all content and settings on Mac https://support.apple.com/HT212749
[MACERASE]	Use Disk Utility to erase a Mac with Apple silicon https://support.apple.com/HT212030
[MACID]	Identify your Mac mini model https://support.apple.com/en-us/HT201894
[MACOSID]	Find out which macOS your Mac is using https://support.apple.com/HT201260
[MACOSSLA]	A. Apple macOS Software License Agreement for macOS Monterey B. Apple Pay Supplemental Terms and Conditions https://www.apple.com/legal/sla/docs/macOSVentura.pdf
[MACOSUPDATE]	How to update the software on your Mac https://support.apple.com/HT201541
[PASSWORD]	Change or reset the password of a macOS user account https://support.apple.com/HT202860
[PERSONAL-SAFETY]	Personal Safety User Guide for Apple devices Set a unique passcode or password on devices https://support.apple.com/en-gb/guide/personal-safety/ipsd0a253dd5/1.0/web/1.0
[PASSWORD_RESET]	Reset your Mac login password https://support.apple.com/guide/mac-help/mh35902/mac
[SEC-ANNOUNCE]	Registration form for Apple security-announce mailing list https://lists.apple.com/mailman/listinfo/security-announce/
[SEC-ISSUE]	Get help with security issues https://support.apple.com/HT201221
[SEC-REPORT]	Report a security or privacy vulnerability https://support.apple.com/HT201220
[SEC-UPDATE]	Apple Security Update https://support.apple.com/HT201222
[SERIAL]	Find the model and serial number of your Mac https://support.apple.com/en-us/HT201581
[SIP]	About System Integrity Protection on your Mac - Apple Support https://support.apple.com/HT204899
[MKSetup]	Set up your Magic Keyboard, Magic Mouse, or Magic Trackpad with your Mac https://support.apple.com/HT201178

[TOUCHID]	Use Touch ID on your Mac https://support.apple.com/guide/mac-help/touch-id-mchl16fbf90a/mac
[TOUCHID_ABOUT]	About Touch ID advanced technology https://support.apple.com/en-us/HT204587

2. Preparation Guidance

After unpacking and powering up the device for the first time, or after a complete erase, the macOS device presents a set of questions to the user as [INITCFG] outlines. Also, [MKSetup] supports users in the Magic Keyboard set up.

As part of the initial configuration, the user is asked to configure a password and enroll into Touch ID, the biometric authentication.

After completion of the initial installation steps, the user shall enroll into Apple Pay. [ENROLLAP] illustrates the enrollment process.

3. Identification

Two guides [MACOSID] and [MACID] are provided for identifying the device model and the installed software:

The following identifiers correspond to the TOEs:

- Model:
 - Mac mini with M2 2023 (Mac14,3)
 - Magic Keyboard with Touch ID (or Magic Keyboard with Touch ID and Numeric Keypad)
- macOS version: macOS Ventura 13.3.1

The part number of Magic Keyboard models included in the TOE start with "MK2".

The firmware version of the keyboard is specified in the Security Target (Section "Target of Evaluation Reference"). It is a combination of:

- Crypto Block firmware version (the field "Trusted Accessory FW version")
- Bluetooth chip firmware version (the field "BTFW Version")
- Keyboard controller firmware version (the field "STFW Version")

These elements can be checked by the user with the following command in Terminal:

```
"ioreg -l | xrn AppleDeviceManagementHIDEventService"
```

```
+--o AppleDeviceManagementHIDEventService <class AppleDeviceManagementHIDEventS$
{
  "IOGeneralInterest" = "IOCommand is not serializable"
  "IOMatchedAtBoot" = Yes
  "LowBatteryNotificationPercentage" = 0x2
  "PrimaryUsagePage" = 0xff00
  "BatteryFaultNotificationType" = "KBBatteryFault"
  "HasBattery" = Yes
  "VendorID" = 0x5ac
  "TrustedAccessoryFW Version" = 0x149e
  "Built-In" = No
  "DeviceAddress" = "9c-58-3c-ed-f0-e5"
  "VersionNumber" = 0x400
  "WakeReason" = "Keyboard (0x02)"
  "Product" = "Magic Keyboard with Touch ID"
  "SerialNumber" = "F0T135600PE0QCMA9"
  "Transport" = "USB"
  "PoweredOnNotificationType" = "USBKB0n"
  "Manufacturer" = "Apple Inc."
  "ConnectionNotificationType" = "USBConnectedKB"
  "ProductID" = 0x29a
  "DeviceUsagePairs" = ({"DeviceUsagePage"=0xff00,"DeviceUsage"=0xb},{"Devi$
  "IOPersonalityPublisher" = "com.apple.driver.AppleTopCaseDriverV2"
  "PoweredOffNotificationType" = "USBKB0ff"
  "BD_ADDR" = <9c583cedf0e5>
  "BatteryPercent" = 0x47
  "BatteryStatusNotificationType" = "BatteryStatusChanged"
  "CriticallyLowBatteryNotificationPercentage" = 0x1
  "ReportInterval" = 0x1f40
  "RadioFW Version" = 0x148
  "VendorIDSource" = 0x0
  "STFW Version" = 0x400
  "CFBundleIdentifier" = "com.apple.driver.AppleTopCaseHIDEventDriver"
  "IOProviderClass" = "IOHIDInterface"
  "LocationID" = 0x1100000
  "BluetoothDevice" = Yes
  "IOClass" = "AppleDeviceManagementHIDEventService"
  "HIDServiceSupport" = No
  "CFBundleIdentifierKernel" = "com.apple.driver.AppleTopCaseHIDEventDriver$
  "ProductIDArray" = (0x29a)
  "BatteryStatusFlags" = 0x3
  "ColorID" = 0x21
  "IOMatchCategory" = "IODefaultMatchCategory"
  "StandardType" = 0x0
  "IOProbeScore" = 0x1c07
  "CountryCode" = 0x0
  "PrimaryUsage" = 0xb
  "BTFW Version" = 0x148
}
```

4. Operational Guidance

In addition to the initial configuration steps, various use cases and options are available for the security functions at runtime. All security related mechanisms are documented as follows.

In general, all security features of macOS devices including authentication, system updates, and Apple Pay are documented in [APS]. In addition, specific user guidance is given in the documents referenced in subsequent sections of this document.

Apple provides a high level document covering the macOS Software License and Agreement [MA-COSSLA]. This document includes supplemental terms and conditions for the use of Apple Pay.

4.1. Configure Password

The configuration user interface for managing the device password is specified at [PASSWORD]. The guidance provides details about adding, changing, and removing a password.

To prevent anyone except the user from using their devices and accessing their information, the user should set a unique passcode or password that only they know. The Personal Safety User Guide [PERSONAL-SAFETY] provides guidance on setting up a passcode or password on devices.

4.2. Check warranty status

The documents [SERIAL] and [CHECK-SERIAL] allow the user to check the warranty status of their Apple devices.

4.3. Configure Touch ID

macOS allows the configuration of Touch ID by allowing users to enroll one or more fingerprints and manage the already enrolled fingerprints, including their removal. All configuration steps pertaining to these actions are given at [TOUCHID].

[TOUCHID] and [TOUCHID_ABOUT] provide information about how Touch ID is used to unlock the device and during Apple Pay transactions.

4.4. Update macOS

The macOS operating system can be updated following the steps provided at [MACOSUPDATE]. macOS updates include all software and firmware relevant to Apple Pay.

4.5. Apple Pay

With Apple Pay, users can enroll credit cards and debit cards to perform transactions using a macOS device. All transactions and usage scenarios that can be performed with Apple Pay are detailed at [AP].

4.6. Operational failures

[PASSWORD_RESET] provides instructions to reset a forgotten password.

4.7. Security Settings

The following macOS Security Settings must **not** be altered from their default values. The default values are as follows:

- System Integrity Protection (SIP): enabled
- Security Policy: "Full Security"

4.8. Security updates, announces and registering

[SEC-ANNOUNCE] allows any user to sign up to be notified about security issues and updates.

[SEC-ISSUE] alerts users about security issues related to their Apple devices and corresponding actions to take.

[SEC-REPORT] provides any person, Apple customer or not, directions to report a security or privacy vulnerability.

[SEC-UPDATE] lists the latest security updates for Apple software products.

4.9. Trusted Root Users

The Apple Pay User is responsible for ensuring that other users of the device with root access are trusted and competent to prevent inadvertent malware installation.

4.10. Erase all content and settings – Disk erase

The Apple Pay User can reset the device content and settings as described in [MACRESET] or completely erase the disk as described in [MACERASE]. This operation will remove any authentication credentials (password and biometric) and mark the Card Data for all the cards enrolled on the device as invalid. A new enrollment is then required to use the cards again on the device.

Annex A – Issuer Security Objectives

For Apple Pay services, the Issuer or its service provider is the third party in charge of:

- Management of user data for Apple Pay services
- Processing Apple Pay transactions

The Issuers authorized to provision cards (for their cardholders, or to the cardholders of their affiliates) enforce the following Security Objectives:

Environment Security Objectives	Description
Cardholder and Apple Pay Perso	The Issuer is responsible for verifying that the User is authorized to perform a transaction on the payment account linked to the card used as a reference, before allowing the card personalization. The Issuer also ensures the robustness of the personalization data, to prevent attacks like forgery, counterfeit, or corruption.
Card Data	The Issuer is responsible for using the appropriate security measures to protect the confidentiality and the integrity of the sensitive card data and for guaranteeing the authenticity of the card data during enrolment.
Card Delete	The Issuer of a payment card provisioned on a device is informed after the User removes the card from that device, removes that device from the iCloud account, or performs a device disk erase. The Issuer ensures the provisioned card is removed from the User's payment account (i.e., the unlinking process of the DPAN from the FPAN, which is done by the Issuer or the corresponding TSP).
Apple Pay Transaction Verification	For Apple Pay, the cryptogram released by the Secure Element for an Apple Pay transaction is verified by the Issuer (or its service provider such as the card scheme). The cryptogram validation result allows the Issuer to approve or reject the transaction. The payment is invalidated if this verification fails.
Statement	The Issuers ensure that the statement associated to the DPAN (list of transactions) is fully accurate and includes, but is not restricted to, the amount and recipient of each transaction.
Dynamic Linking	For eCommerce transactions, the Issuer (or its service provider) verifies the cryptographic based dynamic linking of the transaction data (including amount and payee). The payment is invalidated if this verification fails.

Annex B – Apple Server Security Objectives

Apple servers are in charge of:

- Management of a User's iCloud account
- Management of User enrollment in Apple Pay
- Management of macOS releases
- Device's interface for processing Apple Pay transactions (contact S.Issuer)

Apple servers enforce a range of security objectives:

Environment Security Objectives	Description
Anti-Replay	The Apple Pay server verifies that each payment (e-Commerce Apple Pay transaction) is not replayed. The payment is invalidated if this verification fails.
Dynamic Linking	For eCommerce transactions, the Apple Pay server preserves the cryptographic based dynamic linking of the transaction data (including amount and payee).
Genuine_Wallet	The Wallet application is provided and signed by Apple.

Change History

Date	Version	Author	Comments
2023-02-28	1.0	Apple	Initial version
2023-07-14	1.1	Apple	Minor updates
2023-07-19	1.2	Apple	Minor updates
2023-09-28	1.3	Apple	Minor updates
2023-10-17	1.4	Apple	Minor updates