Strong Customer Authentication for Apple Pay on Mac mini with M2 Pro and Magic keyboard with Touch ID, running macOS Sonoma 14.4

Guidance

Version 4.0
October 1, 2024

Apple
One Apple Park Way
Cupertino, CA 95014

Table of Contents

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 2024
[CHECK-SERIAL]	Check Your Service and Support Coverage (review your Apple warranty status) *https://checkcoverage.apple.com*
[DEVICE_ID]	PSD2 security certifications - Device Identity
[MACESSENTIALS]	Mac mini Essentials *https://support.apple.com/guide/mac-mini/welcome/mac*
[MACID]	Identify your Mac mini model *https://support.apple.com/HT201894*
[MACOSID]	Find out which macOS your Mac is using *https://support.apple.com/HT201260*
[MACOSSLA]	A. Apple macOS Software License Agreement for macOS Sonoma B. Apple Pay Supplemental Terms and Conditions *https://www.apple.com/legal/sla/docs/macOSSonoma.pdf*
[MACOSUPDATE]	How to update the software on your Mac *https://support.apple.com/HT201541*
[MACRESET]	Erase your Mac and reset it to factory settings *https://support.apple.com/102664*
[MKSetup]	Set up your Magic Keyboard, Magic Mouse, or Magic Trackpad with your Mac *https://support.apple.com/HT201178*
[PASSWORD_ERROR]	If you can't reset your Mac login password *https://support.apple.com/HT212190*
[PASSWORD_RESET]	If you forgot your Mac login password *https://support.apple.com/102633*
[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/guide/personal-safety/ipsd0a253dd5/1.0/web/1.0*
[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/HT201581*
[SIP]	About System Integrity Protection on your Mac - Apple Support *https://support.apple.com/HT204899*
[TOUCHID_ABOUT]	About Touch ID advanced technology *https://support.apple.com/HT204587*

[TOUCHID_ERROR]	If Touch ID isn't working on your Mac *https://support.apple.com/HT212225*
[Unlock_Mac_AW]	Unlock your Mac with your Apple Watch *https://support.Apple.com/HT206995*
[USER-GUIDE]	macOS User Guide for macOS Sonoma *https://support.apple.com/guide/mac-help/welcome/mac*

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 and instructions to the user as outlined in the "*Set up your Mac*" Section of [MACESSENTIALS][1]. In addition to the steps outlined in [MACESSENTIALS], the user is required to:

- Select written and spoken languages to be used by the OS and applications, input sources, and for dictation
- Agree to [MACOSSLA], the macOS Software License Agreement (SLA)

In addition, [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 method used by the TOE.

After completion of the initial installation steps, the user shall[2] enroll into Apple Pay. [AP] illustrates the enrollment process.

In order to use the "Unlock with Apple Watch" feature the user needs to perform the configuration steps outlined in [Unlock_Mac_AW].

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:

- TOE: Strong Customer Authentication for Apple Pay, on Mac mini with M2 Pro and Magic keyboard with Touch ID running macOS Sonoma 14.4
- Device Model:
  - Mac mini with M2 Pro 2023
  - Magic keyboard with Touch ID (or Magic keyboard with Touch ID and Numeric Keypad)
- macOS version: macOS Sonoma 14.4
- Safari version: version 17.4 (19618.1.15.11.12)

[1] The user is also prompted to set up Siri and iCloud Keychain (if a new Apple ID is created), however, neither of these features are part of the TOE

[2] Enrolling into Apple Pay is not a mandatory step of the device setup process; however, it is required to install the TOE in its evaluated configuration

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”): 0x5190
- Bluetooth chip firmware version (the field “BTFW Version”): 0x206
- Keyboard controller firmware version (the field “STFW Version”): 0x420

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

“`ioreg -lxrn AppleDeviceManagementHIDEventService`”

```
+-o AppleDeviceManagementHIDEventService  <class AppleDeviceManagementHIDEventS$
    {
      "IOGeneralInterest" = "IOCommand is not serializable"
      "IOMatchedAtBoot" = Yes
      "LowBatteryNotificationPercentage" = 0x2
      "PrimaryUsagePage" = 0xff00
      "BatteryFaultNotificationType" = "KBBatteryFault"
      "HasBattery" = Yes
      "VendorID" = 0x5ac
      "TrustedAccessoryFW Version" = 0x5190
      "Built-In" = No
      "DeviceAddress" = "90-9c-4a-b4-19-38"
      "VersionNumber" = 0x420
      "WakeReason" = "Host (0x01)"
      "Product" = "Magic Keyboard with Touch ID"
      "SerialNumber" = "F0T0413003W0JFW0L"
      "Transport" = "USB"
      "PoweredOnNotificationType" = "USBKBOn"
      "Manufacturer" = "Apple Inc."
      "ConnectionNotificationType" = "USBConnectedKB"
      "ProductID" = 0x29a
      "DeviceUsagePairs" = ({"DeviceUsagePage"=0xff00,"DeviceUsage"=0xb},{"Devi$
      "IOPersonalityPublisher" = "com.apple.driver.AppleTopCaseDriverV2"
      "PoweredOffNotificationType" = "USBKBOff"
      "BD_ADDR" = <909c4ab41938>
      "BatteryPercent" = 0x64
      "BatteryStatusNotificationType" = "BatteryStatusChanged"
      "CriticallyLowBatteryNotificationPercentage" = 0x1
      "ReportInterval" = 0x1f40
      "RadioFW Version" = 0x206
      "VendorIDSource" = 0x0
      "STFW Version" = 0x420
      "CFBundleIdentifier" = "com.apple.driver.AppleTopCaseHIDEventDriver"
      "IOProviderClass" = "IOHIDInterface"
      "LocationID" = 0x2100000
      "BluetoothDevice" = Yes
      "IOClass" = "AppleDeviceManagementHIDEventService"
      "HIDServiceSupport" = No
      "CFBundleIdentifierKernel" = "com.apple.driver.AppleTopCaseHIDEventDriver$
      "ProductIDArray" = (0x29a)
      "BatteryStatusFlags" = 0x3
      "ColorID" = 0x0
      "IOMatchCategory" = "IODefaultMatchCategory"
      "CountryCode" = 0x0
      "IOProbeScore" = 0x1c07
      "PrimaryUsage" = 0xb
      "StandardType" = 0x0
      "BTFW Version" = 0x206
    }
```

The other components of the TOE are tied to the device and macOS versions listed above and are not configurable.

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 [MACOSSLA]. This document includes supplemental terms and conditions for the use of Apple Pay.

The only user role applicable to the TOE is the end user of the device, therefore, the functions and priveleges described in this document apply only to the end user.

There is only one operational mode in the certified configuration of the TOE, resulting from booting macOS with the Security Policy configured for "*Full Security*" as described in Section 4.7 (refer to [APS] for details).

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 the user knows. The Personal Safety User Guide [PERSONAL-SAFETY] provides guidance on setting up a passcode or password on devices.

To discourage brute force password attacks, there are escalating time delays after the entry of an invalid password at the Lock Screen, as specified in the Security Target (FIA_AFL.1/Delay Authentication failure handling).

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 in [USER-GUIDE], Section "Use Touch ID".

The [USER-GUIDE] ("Use Touch ID on Mac" section) and the [TOUCHID_ABOUT] document 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.

[PASSWORD_ERROR] provides steps the User should follow if password reset fails.

[TOUCHID_ERROR] provides steps the User should follow if Touch ID is not working.

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"

User guidance for the configuration of the macOS system security settings is described in more detail in the "*Set up your Mac*" Section of [MACESSENTIALS].

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

The Apple Pay User can reset the device content and settings as described in [MACRESET]. 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.

4.11. Apple Watch

[Unlock_Mac_AW] allows the user to unlock their device and approve other requests to enter their administrator password using a paired Apple Watch.

Annex A – Card issuer Security Objectives

For Apple Pay services, the card 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 card 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 card 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 card issuer also ensures the robustness of the personalization data, to prevent attacks like forgery, counterfeit, or corruption.
Card Data	The card 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 card 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 card 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 card 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 card issuer (or its service provider such as the payment network). The cryptogram validation result allows the card issuer to approve or reject the transaction. The payment is invalidated if this verification fails.
Statement	The card 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 card 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.

Annex C – Apple Watch Security Objectives

Apple Watch is responsible for:

- Protecting the confidentiality of the unlock secret of the Mac mini
- Preventing unauthorized access to the “Unlock Mac with Apple Watch” feature

Apple Watch enforces the following security objective:

Environment Security Objectives	Description
Watch	The Apple Watch is responsible for ensuring the confidentiality of the unlock secret provided by the Mac mini during all its lifetime: from its reception at enabling of the “Unlock with Apple Watch” feature, during its storage, during its release for unlocking the Mac mini, and when it is deleted when the feature is disabled. The Apple Watch is responsible for ensuring that it is protected by a password and the wrist detection feature is turned on in order to enable the feature “Unlock Mac with Apple Watch”.

Annex D – User Security Objectives

The user of the TOE is responsible for:

- Taking appropriate measures to control access to the TOE
- Controlling which devices pair with the TOE

The user enforces the following security objective:

Environment Security Objectives	Description
User	The User is responsible for ensuring that: • Other users of the device with root access are trusted and competent to prevent inadvertent malware installation • They authorize all the Apple Pay activities that are performed on the device • The password is robust and protected • Only their own biometrics credentials are enrolled (they do not enroll biometrics of someone else) • The Mac mini is only paired with the Magic keyboard with Touch ID, the Mac mini is not paired with any other keyboard • Only their own Apple Watch is paired with the Mac mini and the paired Apple Watch is protected. This includes abiding by the watchOS Software License Agreement and protecting the confidentiality of the paired Apple Watch's passcode

Change History

Date	Version	Author	Comments
2024-03-31	1.0	Apple	Initial version
2024-04-26	2.0	Apple	Minor updates
2024-06-07	3.0	Apple	Minor updates
2024-10-01	4.0	Apple	Minor updates