

Strong Customer Authentication for Apple Pay on MacBook Air 2022 with M2 running macOS Ventura 13.3.1

Guidance

Version 1.6

November 16, 2023

Table of Contents

1. Introduction	3
2. Preparation Guidance	4
3. Identification	4
4. Operational Guidance	4
4.1. Configure Password	5
4.2. Check warranty status	5
4.3. Configure Touch ID	5
4.4. Update macOS	5
4.5. Apple Pay	5
4.6. Operational failures	5
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	6
4.11. Apple Watch	6
Annex A - Issuer Security Objectives	7
Annex B – Apple Server Security Objectives	8
Annex C – Apple Watch Security Objectives	9
Annex D – User Security Objectives	10

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
[DEVICE_ID]	PSD2 security certifications 2023 Device Identity
[INITCFG]	Set up your MacBook Air https://support.apple.com/guide/macbook-air/set-up-your-mac-apd831707cb3/mac
[INITCFG_NEW_USER]	Set up your MacBook Air for new Mac users https://support.apple.com/en-gb/guide/macbook-air/apd3a3bbbed27/2023/mac/13.4
[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 MacBook Air model https://support.apple.com/HT201862
[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
[PASSWORD_ERROR]	If you can't reset your Mac login password https://support.apple.com/HT212190
[PASSWORD_RESET]	Reset your Mac login password https://support.apple.com/guide/mac-help/mh35902/mac
[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
[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
[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
[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

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] and [INITCFG_NEW_USER] outlines.

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. **Error! Reference source not found.** 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:

- TOE: Strong Customer Authentication for Apple Pay, on MacBook Air 2022 with M2 running macOS Ventura 13.3.1
- Device Model: MacBook Air 2022 with M2
- macOS version: macOS Ventura 13.3.1
- Safari version: Version 16.4 (18615.1.26.11.23)

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

The protection of the integrity and authenticity of the delivered TOE (i.e. detection that the TOE has not been modified during delivery) is described in [DEVICE_ID].

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 privileges 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 they know. 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 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.

[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 [INITCFG].

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.

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 - 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.

Annex C – Apple Watch Security Objectives

Apple Watch is responsible for:

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

Apple Watch enforces the following security objective:

Environment Se- curity Objec- tives	Description
Watch	<p>The Apple Watch is responsible for ensuring the confidentiality of the unlock secret provided by the MacBook Air 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 MacBook Air, and when it is deleted when the feature is disabled.</p> <p>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”.</p>

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 Se- curity Objec- tives	Description
User	<p>The User is responsible for ensuring that:</p> <ul style="list-style-type: none">• Other users of the device with root access are trusted and competent to prevent inadvertent malware installation• They own 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 TOE is not paired with an external keyboard• Only their own Apple Watch is paired with the TOE 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
2023-02-28	1.0	Apple	Initial version
2023-07-24	1.1	Apple	Updates in response to Observation Report (OR)
2023-08-07	1.2	Apple	Updates in response to OR
2023-09-22	1.3	Apple	Updates in response to OR
2023-10-06	1.4	Apple	Minor updates
2023-10-17	1.5	Apple	Minor updates
2023-11-16	1.6	Apple	Updates in response to OR