Strong Customer Authentication for Apple Pay on MacBook Air 2020 with M1 running macOS Monterey 12.3.1

Guidance

Version 1.4
November 11, 2022

Apple
One Apple Park Way
Cupertino, CA 95014

Copyright © 2022 Apple Inc. All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

Table of Contents

Copyright © 2022 Apple Inc. All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

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 *https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf*
[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 MacBook Air *https://support.apple.com/guide/macbook-air/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 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/macOSMonterey.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-ISSUES]	Get help with security issues *https://support.apple.com/HT201221*
[SEC-REPORT]	Report a security or privacy vulnerability *https://support.apple.com/HT201220*
[SEC-UPDATES]	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*

Copyright © 2022 Apple Inc. All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

[TOUCHID]	Use Touch ID on your Mac *https://support.apple.com/guide/mac-help/touch-id-mchl16fbf90a/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 to the user as [INITCFG] 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 is able to 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: MacBook Air 2020
- macOS version: 12.3.1

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.

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.

Copyright © 2022 Apple Inc. All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

4.2. Check warranty status

The documents [SERIAL] and [CHECK-SERIAL] allow any user to check 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 andmanage the already enrolled fingerprints, including their removal. All configuration steps pertaining to these actions are given at [TOUCHID].

This guidance documentation also provides 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-ISSUES] 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-UPDATES] lists the last security updates for Apple software products.

Copyright © 2022 Apple Inc. All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

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 setting with [MACRESET] or completely erase the disk with [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 (new enrollment is required to use again the card on the device).

Copyright © 2022 Apple Inc. All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

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 card holders, or to the card holders of their affiliates) enforce the following Security Objectives:

Environment Security Objectives	Description
Card Holder and Apple Pay Perso	The Issuer is responsible for verifying that the User is authorized to perform a transaction on the account of 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 guaranteeing the authenticity of the card data during enrolment.
Card Delete	The Issuers of all payment cards provisioned on a device are informed after the User removes a card from that device, removes that device from the iCloud account or performs a device disk erase. The Issuers ensure these cards are 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). The cryptogram validation result allows the Issuer to approve or reject the transaction. The payment is invalidated if this verification fails.
Statement	The payment card Issuers ensure that the statement associated to the card (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 verifies the cryptographic based dynamic linking of the transaction data (including amount and payee). The payment is invalidated if this verification fails.

Copyright © 2022 Apple Inc. All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

Annex B - Apple Server Security Objectives

Apple servers 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.

Copyright © 2022 Apple Inc. All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.

Change History

Date	Version	Author	Comments
2022-02-18	1.0	Apple	Initialization of the document
2022-05-30	1.1	Apple	Minor updates
2022-09-20	1.2	Apple	Minor updates
2022-09-26	1.3	Apple	Minor updates
2022-11-11	1.4	Apple	Minor updates

Copyright © 2022 Apple Inc. All rights reserved.
This document may be reproduced and distributed only in its original entirety without revision.