Strong Customer Authentication for Apple Pay on iPhone 15 Pro with A17 Pro running iOS 17.4

Guidance

Version 3.0

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*
[APC]	Apple Cash Support *https://support.apple.com/apple-cash*
[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
[DISABLE]	If you forgot your iPhone passcode *https://support.apple.com/HT204306*
[FACEID]	Use Face ID on your iPhone *https://support.apple.com/HT208109*
[FACEID_ABOUT]	About Face ID advanced technology *https://support.apple.com/HT208108*
[FACEID_ISSUE]	Face ID not working on iPhone *https://support.apple.com/HT208114*
[INITCFG]	Set up your iPhone *https://support.apple.com/HT202033*
[IOSID]	Find the software version on your iPhone *https://support.apple.com/HT201685*
[IOSSLA]	A. Apple iOS Software License Agreement B. Apple Pay Supplemental Terms and Conditions *https://www.apple.com/legal/sla/docs/iOS17_iPadOS17.pdf*
[IOSUPDATE]	Update the iOS on your iPhone *https://support.apple.com/HT204204*
[IPHONEID]	Identify your iPhone model *https://support.apple.com/HT201296*
[PASSCODE]	Use a passcode with your iPhone *https://support.apple.com/HT204060*
[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 updates *https://support.apple.com/HT201222*
[SERIAL]	Find the serial number of your iPhone *https://support.apple.com/HT204073*
[Unlock_iPhone_AW]	Unlock your iPhone with Apple Watch *https://support.apple.com/guide/watch/apd2a4393dc1/watchos*

Reference	Description
[USER_GUIDE]	iPhone User Guide *https://support.apple.com/guide/iphone/welcome/ios*

2. Preparation Guidance

After unpacking and powering up the device for the first time, or after a complete erase, the iOS device presents a set of questions to the user as outlined in [INITCFG].

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

After completion of the initial installation steps, the user shall[1] enroll into Apple Pay and can elect to enroll into Apple Cash (if available). The enrollment process is illustrated at [AP]. To enable Apple Cash, the guidance given at [APC] should be consulted.

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

3. Identification

Two guides [IPHONEID] and [IOSID] are provided for identifying the device model and the installed software.

The following identifiers correspond to the TOE:

- TOE: Strong Customer Authentication for Apple Pay, on iPhone 15 Pro with A17 Pro running iOS 17.4
- Device Model: iPhone 15 Pro
- iOS version: iOS 17.4
- Safari version: version 17.4 (19618.1.15)

The other components of the TOE are tied to the device and iOS 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 iOS devices including authentication, system updates, Apple Pay, and Apple Cash 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 iOS Software License and Agreement [IOSSLA], including supplemental terms and conditions for the use of Apple Pay services (Apple Pay and Apple Cash).

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.

[1] 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

There is only one operational mode in the certified configuration of the TOE.

4.1. Configure Passcode

Managing the passcode is provided with the configuration user interface specified in [PASSCODE]. The guidance provides details about adding, changing, and removing a passcode.

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] and the "Privacy and security" section of [USER_GUIDE] provides guidance on setting up a passcode or password on devices.

To discourage brute force passcode attacks, there are escalating time delays after the entry of an invalid passcode, 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 Face ID

iOS allows the configuration of Face ID by allowing users to enroll their face (up to two enrollments if the user enables the use of an alternate appearance), and removal of all enrolled faces. All configuration steps pertaining to these actions are given in [FACEID] and the "Privacy and security" section of [USER_GUIDE].

[FACEID] and [FACEID_ABOUT] provide information about how Face ID is used to unlock the device and during Apple Pay and Apple Cash transactions.

4.4. Update iOS

The iOS operating system can be updated following the steps provided in [IOSUPDATE].

iOS updates include all software and firmware relevant to Apple Pay and Apple Cash.

4.5. Apple Pay

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

Security Note: The User SHALL NEVER perform Apple Pay card provisioning on a device that is plugged into another piece of equipment.

4.6. Apple Cash

Apple Cash allows several different operations, including payments and transfer of money from a debit card to Apple Cash. All aspects related to Apple Cash are documented in [APC].

4.7. Operational failures

Two guides [FACEID_ISSUE] and [DISABLE] are provided for handling the device in cases where:

- Face ID does not work
- The User forgets their passcode
- The device is disabled

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. Apple Watch

[Unlock_iPhone_AW] allows the user to unlock their device using a paired Apple Watch.

Annex A - Card issuer Security Objectives

For Apple Pay services (Apple Pay and Apple Cash), the card issuer or its service provider is the third party in charge of:

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

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/Apple Cash 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 Erase All Content and Settings. 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	For Apple Pay, 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. For Apple Cash, the payment card issuer ensures that the ledger associated to an Apple Cash account (list of transfers including completed/canceled/pending) is fully accurate.
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.
CDCVM	Payment networks or card issuers are responsible for ensuring that Express transactions can only be accepted for transit-specific use by requiring that non-transit Apple Pay payment transactions have a successful CDCVM.

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 User enrollment in Apple Cash
- Management of iOS releases
- Device's interface for processing Apple Pay transactions (contact S.Issuer)
- Device's interface for processing Apple Cash transfers (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 or Apple Cash transfer) is not replayed. The payment is invalidated if this verification fails.
Apple Cash Transaction Verification	The Apple Pay server ensures that no Apple Cash transfer can be executed if the submitted quote (received by the server before the User approves) does not match the transaction data (received by the server once the device completes transfer processing). The modifications that the server is able to detect cover but are not limited to, modification on the amount and the recipient.
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 Apple 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 iPhone 15 Pro
- Preventing unauthorized access to the “Unlock 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 iPhone 15 Pro during all its lifetime: from its inception at enabling of the “Unlock with Apple Watch” feature, during its storage, during its release for unlocking the iPhone 15 Pro, and when it is deleted when the feature is disabled. The Apple Watch is responsible for ensuring that it is protected by a passcode and the wrist detection feature is turned on in order to enable the feature “Unlock 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: - They authorize all the Apple Pay/Cash activities that are performed on the device - The passcode is robust and protected - Only their own biometrics credentials are enrolled (they do not enroll biometrics of someone else) - 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
2024-03-31	1.0	Apple	Initial version
2024-06-07	2.0	Apple	Minor updates
2024-10-01	3.0	Apple	Minor updates