Strong Customer Authentication for Apple Pay on Apple Watch with S8 running watchOS 9.4

Guidance

Version 1.2
October 17, 2023

Table of Contents

1. Introduction

This document contains references to other documents providing guidance for all 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 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
[DISABLE]	If you forgot your Apple Watch passcode https://support.apple.com/en-us/HT204567
[ENROLLAP]	Set up Apple Pay https://support.apple.com/en-us/HT204506
[ENROLLAPC]	Set up Apple Cash https://support.apple.com/en-us/HT207886
[INITCFG]	Set up your Apple Watch https://support.apple.com/en-us/HT204505
[PERSONAL-SAFETY]	Personal Safety User Guide for Apple devices Set a unique passcode or password on devices https://support.apple.com/en-us/guide/personal-safety/ipsd0a253dd5/1.0/web/1.0
[RESTART]	Restart your Apple Watch https://support.apple.com/en-us/HT204510
[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]	How to find the serial number or IMEI for your Apple Watch https://support.apple.com/en-us/HT204520
[UNLOCK]	Lock or Unlock Apple Watch https://support.apple.com/guide/watch/apd0e1e73b6f/watchos
[WATCHID]	Identify your Apple Watch https://support.apple.com/en-us/HT204507
[WATCHOSID]	See information about Apple Watch https://support.apple.com/guide/watch/apdac6807516/watchos
[WATCHOSSLA]	A.watchOS Software License Agreement B.Apple Pay Supplemental Terms and Conditions https://www.apple.com/legal/sla/docs/watchOS9.pdf
[WATCHOSUPDATE]	Update your Apple Watch https://support.apple.com/en-us/HT204641

2. Preparation Guidance

After either unpacking and powering up the device for the first time, or after a complete erase, the watchOS 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.

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

3. Identification

Two guides [WATCHID] and [WATCHOSID] are provided for identifying the device model and the installed software.

The following identifiers correspond to the TOE:

- Model: Apple Watch S8
- watchOS version: watchOS 9.4

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 watchOS devices including authentication, system updates, Apple Pay, and Apple Cash are documented in [APS] sections “Apple Watch” and “Apple Pay” In addition, specific user guidance is given in the documents referenced in the subsequent sections of this document.

Apple provides a high-level document covering the watchOS Software License and Agreement [WATCHOSSLA] including supplemental terms and conditions for the use of Apple Pay services (Apple Pay and Apple Cash).

4.1. Configure Passcode

Managing the passcode is provided with the configuration user interface specified in [INITCFG]. 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 they know. The Personal Safety User

Guide [PERSONAL-SAFETY] and the “Lock or Unlock” section of the Apple Watch User Guide [UNLOCK] provide 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 Unlock

The Apple Watch can be configured to be unlocked when the paired iPhone is unlocked. Guidance on this configuration is provided in [UNLOCK].

4.4. Update watchOS

The watchOS operating system can be updated following the steps provided in [WATCHOSUPDATE].

watchOS 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 a watchOS mobile device. All transactions and usage scenarios that can be performed with Apple Pay are detailed in [AP].

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 [DISABLE] and [RESTART] are provided for handling the device in case:

- The User forgets the passcode
- The device is not responding

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.

Annex A – Issuer Security Objectives

For Apple Pay services (Apple Pay and Apple Cash), the 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 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 Issuer is responsible for verifying that the device 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 Erase All Content and Settings. 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	For Apple Pay, 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. 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 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 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 watchOS 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.

Change History

Date	Version	Author	Comments
2023-02-28	1.0	Apple	Initial version
2023-09-28	1.1	Apple	Minor updates
2023-10-17	1.2	Apple	Minor updates