

Strong Customer Authentication for Apple Pay on Apple Watch with S4 running watchOS 7.4.1

Guidance

Version 1.3

May 10, 2022

Table of Contents

1	Introduction	1
2	Prerequisites	2
3	Configuration	3
4	Operational failures	4
4.1	Configure Passcode	4
4.2	Configure Unlock	4
4.3	Update watchOS	4
4.4	Apple Pay	4
4.5	Apple Cash	4
4.6	Operational failures	4
5	Appendix	5
5.1	Apple Pay	5
5.2	Apple Cash	5

1. Introduction

This document contains references to other documents providing guidance for all security related topics specified in the Security Target.

Reference	Description
[APC]	Send and receive money with Apple Cash https://support.apple.com/explore/apple-pay-cash
[AP]	Apple Pay Support https://support.apple.com/apple-pay
[ENROLLAP]	Set up Apple Pay https://support.apple.com/en-us/HT204506
[ENROLLAPC]	Set up Apple Cash and person to person payments https://support.apple.com/en-us/HT207886
[INITCFG]	Set up your Apple Watch https://support.apple.com/en-us/HT204506
[APS]	Apple Platform Security https://manuals.info.apple.com/MANUALS/1000/MA1902/en_US/apple-platform-security-guide.pdf
[WATCH-OSUPDATE]	Update your Apple Watch https://support.apple.com/en-us/HT204641
[UNLOCK]	Unlock Apple Watch https://support.apple.com/en-gb/guide/watch/apd0e1e73b6f/watchos
[WATCHOSSLA]	A. watchOS Software License Agreement B. Apple Pay Supplemental Terms and Conditions https://www.apple.com/legal/sla/docs/watchOS7.pdf
[WATCHID]	Identify your Apple Watch model https://support.apple.com/en-us/HT204507
[WATCHSN]	How to find the Serial number https://support.apple.com/en-us/HT204520
[DISABLE]	If you forgot your Apple Watch passcode https://support.apple.com/en-us/HT204567
[RESTART]	How to restart your Apple Watch https://support.apple.com/en-us/HT204510

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 is able to enroll into Apple Pay and Apple Cash. The enrollment process for Apple Pay is illustrated at [ENROLLAP]. To enable Apple Cash, the guidance given at [ENROLLAPC] should be consulted.

3. Identification

The guides [WATCHID] [WATCHSN] are provided for identifying the device model. The version identification can be found on the Apple Watch:

- 1/2 Settings App
- 1/2 General/About Menu
- 1/2 Scroll to Model and Version fields

The following identifiers correspond to the TOE:

- 1/2 Model: Apple Watch Series 4 models: A1975, A1976, A1977, A1978, A2007, and A2008
- 1/2 watchOS version: 7.4.1 (18T201)

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.

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.

When using Apple Pay the user should select a complex passcode and protect it well. They should avoid writing it down and using obvious values such as date of birth that a third party might guess.

4.2. 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].

4.3. 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.

4.4. 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].

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

4.5. Apple Cash

Apple Cash allows a number of 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].

4.6. Operational failures

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

- 🔧 User forgets the passcode
- 🔧 Device is not responding

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:

- ½ Management of user data for Apple Pay services
- ½ Management of user data for Apple Cash services
- ½ Processing Apple Pay transactions
- ½ Processing Apple Cash transfers

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/Apple Cash Perso	The Issuer is responsible for verifying that the device User is authorized to perform a transaction on the account of the card used as a reference, before allowing the Apple Pay/Apple Cash 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 card data during enrolment.
Card Delete	The Issuers of all payment cards provisioned on a device are informed when the User removes a card from that device, removes that device from the iCloud account or performs a device Erase All Content and Settings. The Issuers ensure these cards are removed from the User's 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	For Apple Pay, 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. 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 server 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:

- 1/2 Management of a User's iCloud account
- 1/2 Management of User enrollment in Apple Pay
- 1/2 Management of User enrollment in Apple Cash
- 1/2 Management of watchOS releases
- 1/2 Device's interface for processing Apple Pay transactions (contact S.Issuer)
- 1/2 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 Wallet application is provided and signed by Apple.

Change History

Date	Version	Author	Comments
2021-03-15	1.0	Apple	Initialization of the guidance
2021-08-12	1.1	Apple	Updates for watchOS 7.4.1
2021-11-23	1.2	Apple	Minor fixes
2022-05-10	1.3	Apple	Updates according to internal reviews