

# Strong Customer Authentication for Apple Pay on Vision Pro with M2 running visionOS 2.4

## Security Target

---

Version 1.2  
June 16, 2025

Apple  
One Apple Park Way  
Cupertino, CA 95014

# Table of Contents

- 1. Introduction ..... 4**
  - 1.1. Purpose ..... 4**
  - 1.2. Abbreviations ..... 4**
- 2. ST Introduction ..... 5**
  - 2.1. Security Target Reference ..... 5**
  - 2.2. Target of Evaluation Reference ..... 5**
  - 2.3. TOE Overview ..... 7**
  - 2.4. TOE Description ..... 8**
  - 2.5. Description of the Apple Pay Service ..... 12**
  - 2.6. TOE Use Cases ..... 20**
- 3. Evaluation Assurance ..... 22**
  - 3.1. Common Criteria Reference ..... 22**
  - 3.2. CC Conformance claim ..... 22**
  - 3.3. Protection Profile Conformance claim ..... 22**
  - 3.4. Assurance Level ..... 22**
- 4. Security Problem Definition ..... 24**
  - 4.1. Assets ..... 24**
  - 4.2. Subjects ..... 25**
  - 4.3. Assumptions ..... 26**
  - 4.4. Threat Agents ..... 26**
  - 4.5. Threats ..... 27**
  - 4.6. Organizational Security Policies ..... 29**
- 5. Security Objectives ..... 30**
  - 5.1. Security Objectives for the TOE ..... 30**
  - 5.2. Security Objectives for the environment ..... 31**
  - 5.3. Rationale of the Security objectives for the security problem definition ..... 32**
- 6. Security Functional Requirements ..... 36**
  - 6.1. SFR supporting definitions ..... 36**
  - 6.2. Identification and authentication ..... 37**
  - 6.3. Access/Flow Control SFRs ..... 39**
  - 6.4. Secure Enclave/Secure Element Trusted Channel ..... 42**
  - 6.5. Secure Enclave/iPhone Trusted Channel ..... 42**

6.6. Local data protection .....43

6.7. TSF management .....44

6.8. Security Requirements Rationale .....45

7. TOE Summary Specification ..... 49

7.1. SF User authentication and management .....49

7.2. SF Biometric/Secure Enclave secure channel.....52

7.3. SF Secure Enclave/Secure Element secure channel .....52

7.4. SF Secure Enclave/iPhone secure channel.....52

7.5. SF Card Data management .....53

7.6. SF Payment management .....54

7.7. SF OS Update .....55

7.8. SF iCloud logout & Device reset.....55

# 1. Introduction

## 1.1. Purpose

The purpose of this document is to define the Target of Evaluation (TOE) for meeting the requirements of Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2) and the Commission Delegated Regulation (EU) 2018/389 of 27 November 2017, focusing on the Strong Customer Authentication and Dynamic Linking for Apple Pay.

## 1.2. Abbreviations

Abbreviation	Meaning
<b>AP</b>	Application Processor
<b>API</b>	Application Programming Interface
<b>AR</b>	Authorization Random
<b>CDCVM</b>	Consumer Device Cardholder* Verification Method
<b>CL</b>	Contactless
<b>CRS</b>	Contactless Registry Service
<b>CVV</b>	Card Verification Value
<b>HSM</b>	Hardware Security Module
<b>I/O</b>	Input / Output
<b>MAC</b>	Message Authentication Code
<b>NFC</b>	Near Field Communication
<b>OS</b>	Operating System
<b>PNO</b>	Payment Network Operator
<b>PSD2</b>	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015
<b>SCA</b>	Strong Customer Authentication
<b>SIP</b>	System Integrity Protection
<b>SKS</b>	Secure Key Store
<b>SSE</b>	An application in the Secure Enclave managing the pairing between the Secure Enclave and the Secure Element
<b>TSM</b>	Trusted Service Manager
<b>TSP</b>	Token Service Provider
<b>UID</b>	Unique Identifier

\* refers to the Apple Pay user.

## 2. ST Introduction

### 2.1. Security Target Reference

This Security Target is identified with the following information:

Security Target identifiers	
<b>Title</b>	Strong Customer Authentication for Apple Pay on Vision Pro with M2 running visionOS 2.4, Security Target
<b>Version</b>	1.2
<b>Date</b>	June 16, 2025
<b>Developer</b>	Apple Inc.

### 2.2. Target of Evaluation Reference

TOE identifier
Strong Customer Authentication for Apple Pay on Vision Pro with M2 running visionOS 2.4

The Target of Evaluation (TOE) platform is a Vision Pro with M2 running visionOS 2.4, with the following platform identifiers:

Platform identifiers	
<b>Device</b>	Vision Pro with M2
<b>Operating System</b>	visionOS 2.4 (Build 22O238)
<b>Developer</b>	Apple Inc.

The TOE consists of a range of hardware and software components as listed below, which are all developed by Apple.

TOE Component	Version	Description
<b>Apple Wallet App (Wallet)</b>	App part of visionOS 2.4	Authentication policy on data and services In-app transaction data management
<b>Application Processor (AP)<sup>1</sup></b>	M2	Authentication policy on data and services In-app transaction data management
<b>Optic ID</b>	Onboard cameras and LEDs for iris recognition within Vision Pro	Hardware and associated drivers for iris data capture and secure transfer to BioApp to allow for enrollment and matching

<sup>1</sup> Only the parts of the AP related to the TSF are included within the TOE scope. The GPU of the AP is not relevant to the TSF and is therefore not part of the TOE.

TOE Component	Version	Description
<b>Boot Loader</b>	visionOS 2.4	Allows the device to start and boot the operating system
<b>Secure Enclave</b>	sepOS part of visionOS 2.4	Authentication Setup: <ul style="list-style-type: none"> <li>• Enrollment of the authentication material</li> <li>• User authentication verification</li> </ul> Authentication Prover: <ul style="list-style-type: none"> <li>• Passcode verification</li> <li>• Biometrics matching</li> <li>• Authentication policy on data</li> </ul>
• <b>SSE</b>		Manages the pairing between the Secure Enclave and the Secure Element
• <b>SKS</b>		Hardware Cryptographic module
• <b>BioApp</b>		Provides functionality for processing biometric data and generating biometric templates
<b>visionOS Platform</b>	Device operating system platform (visionOS 2.4) executing on Application Processor (AP) with the following Apple Pay services that are included in the TOE:	
• Security Framework	visionOS 2.4	Provides functionality to protect information, establish trust, and control access to software
• NFCd	visionOS 2.4	Provides communication layer between the TOE and the Secure Element
• Safari	visionOS 2.4	Browser
• Settings	visionOS 2.4	Allows the user to indicate their preferred settings for the device, operating system, and applications
• UI boards	visionOS 2.4	Provides the functionality for the visionOS user interface
<b>Console</b>	Display and sensors of the Vision Pro  Device drivers of visionOS 2.4	Display and sensors of the Vision Pro, which provide the input/output (I/O) functionality

The Secure Element of the device is separately certified according to the Common Criteria and is therefore out of scope of this evaluation.

*Note: In the evaluated configuration the cryptographic modules are supplied by Apple as part of visionOS and sepOS. Readers may draw some assurance from the conformance to FIPS 140-3 certified by the Cryptographic Module Validation Program for corecrypto for each major release (Apple corecrypto User Space Module, Apple corecrypto Kernel Space Module and the Apple Secure Key Store Cryptographic Module).*

*Additionally, the browser, Safari, is evaluated for each major OS release using the collaborative PP (cPP), Protection Profile for Application Software Version 1.3.*

The TOE guidance document is listed in the following table.

Apple Pay Guidance	Reference	Version
Strong Customer Authentication for Apple Pay on Vision Pro with M2 running visionOS 2.4: Guidance	[AGD]	1.1

## 2.3. TOE Overview

### 2.3.1. TOE type

The TOE is a combination of Hardware and Software components that implement Strong Customer Authentication and Dynamic Linking for Apple Pay on the Vision Pro with M2 running visionOS 2.4.

### 2.3.2. TOE usage and major security features

The TOE includes the components implementing Strong Customer Authentication (SCA) and Dynamic Linking for Apple Pay. The TOE is the Vision Pro with M2 running visionOS 2.4 operating system.

The operating system manages the device hardware, provides Apple Pay and Apple Cash functionalities, and provides the technologies required to enforce Strong Customer Authentication and Dynamic Linking for Apple Pay and Apple Cash e-commerce transactions. Dynamic Linking for a transaction is the link between the authentication code generated upon successful SCA, with both the transaction's original specific amount and the identity of the payee.

The operating system provides a consistent set of capabilities allowing the supervision of enrolled devices. This includes the preparation of devices for deployment, the subsequent management of the devices, and the termination of management.

The TOE platform protects itself by having its own code and data protected from unauthorized access (using hardware provided memory protection features), by securing user and TOE Security Functionality (TSF) data, by ensuring the integrity and authenticity of TSF updates and downloaded applications, and by locking the TOE when the user takes off the device.

The TOE provides protection of data at rest, and access control mechanisms for use by applications. Access control for data and services, including Apple Pay and Apple Cash, rely on the enforcement of user authentication.

To use Apple Pay, a user must have a passcode set on the device and, optionally, biometrics (Optic ID). User authentication to authorize an Apple Pay transaction on an enrolled device is provided by a user-defined passcode and the user enrolled biometrics. The minimum length of the passcode, passcode rules, and the maximum number of consecutive failed authentication attempts is statically set by Apple for each OS release. Biometrics are enrolled and managed by the user. Optic ID is designed to confirm user attention using gaze tracking and provide robust authentication with a low false-match rate, and mitigate both digital and physical spoofing.

The Secure Enclave is responsible for ensuring user authorization (the combination of user authentication and user intent) before a payment is authorized from the device.

### 2.3.3. Non-TOE hardware/software/firmware

The TOE environment includes the Secure Element (Hardware, Operating System, CRS applet and payment applets in the Secure Element) and the NFC communication layer (the NFC Controller (NFCC)).

The Secure Element is included in the device but is outside the scope of the TOE boundary and is separately evaluated to Common Criteria. The Secure Element is contained in the same package as the NFCC. Payment applets in the Secure Element manage the payment process for Apple Pay transactions. The NFCC is not connected to any antenna and is thus not usable for NFC transactions. It is used only for communications between the TOE and the Secure Element.

The TOE relies on its environment to facilitate Apple Pay transactions (and Apple Cash transfers); the transaction data is always processed by the Secure Element. The Secure Element only allows payment data to be sent from the device after it receives authorization from the Secure Enclave. For each transaction, the payment applets hosted on the Secure Element generate a payment cryptogram. This cryptogram and the Device Account Number form a transaction-specific dynamic security code, which is sent from the device to the card issuer (or its tokenization service provider such as a payment network) to use to verify each transaction.

The subsystems of the TOE are listed in Section 2.4 of this Security Target. All other components and subsystems of visionOS (including user space and kernel software), hardware and subsystems included in the device (including the camera and networking subsystems), and the paired iPhone are all considered to be part of the TOE environment. The networking subsystem provides connectivity to the Apple servers responsible for managing Apple Pay transactions and to the iPhone.

The “Nearby iPhone enables Optic ID” feature relies on a secure pairing process between the TOE and the iPhone, and a secure unlock process thereafter.

## 2.4. TOE Description

### 2.4.1. TOE Architecture

The TOE platform includes the components implementing Strong Customer Authentication (SCA) and dynamic linking for Apple Pay.

User authentication is managed by the Secure Enclave. The Secure Enclave is a dedicated secure subsystem integrated into Apple systems on chip (SoCs). The Secure Enclave is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even if the Application Processor kernel were to be compromised.

visionOS allows the Apple Pay services and other security functions of the TOE to operate.

The Secure Element (outside of the TOE) is the secure component that holds the Apple Pay secrets and processes the Apple Pay transactions.

The guidance documentation of the TOE is listed in the *Apple Pay Guidance* table of section 2.2.

The identifiers of the TOE components are given in the *TOE Component* table of section 2.2.



The distribution channels for Users to obtain the devices include:

- The “Apple Store” which is either physical store or online store at <https://www.apple.com>
- Apple retailer
- Resellers
- Other specific channels for Government and business

The component parts of the TOE are shown in Figure 1.

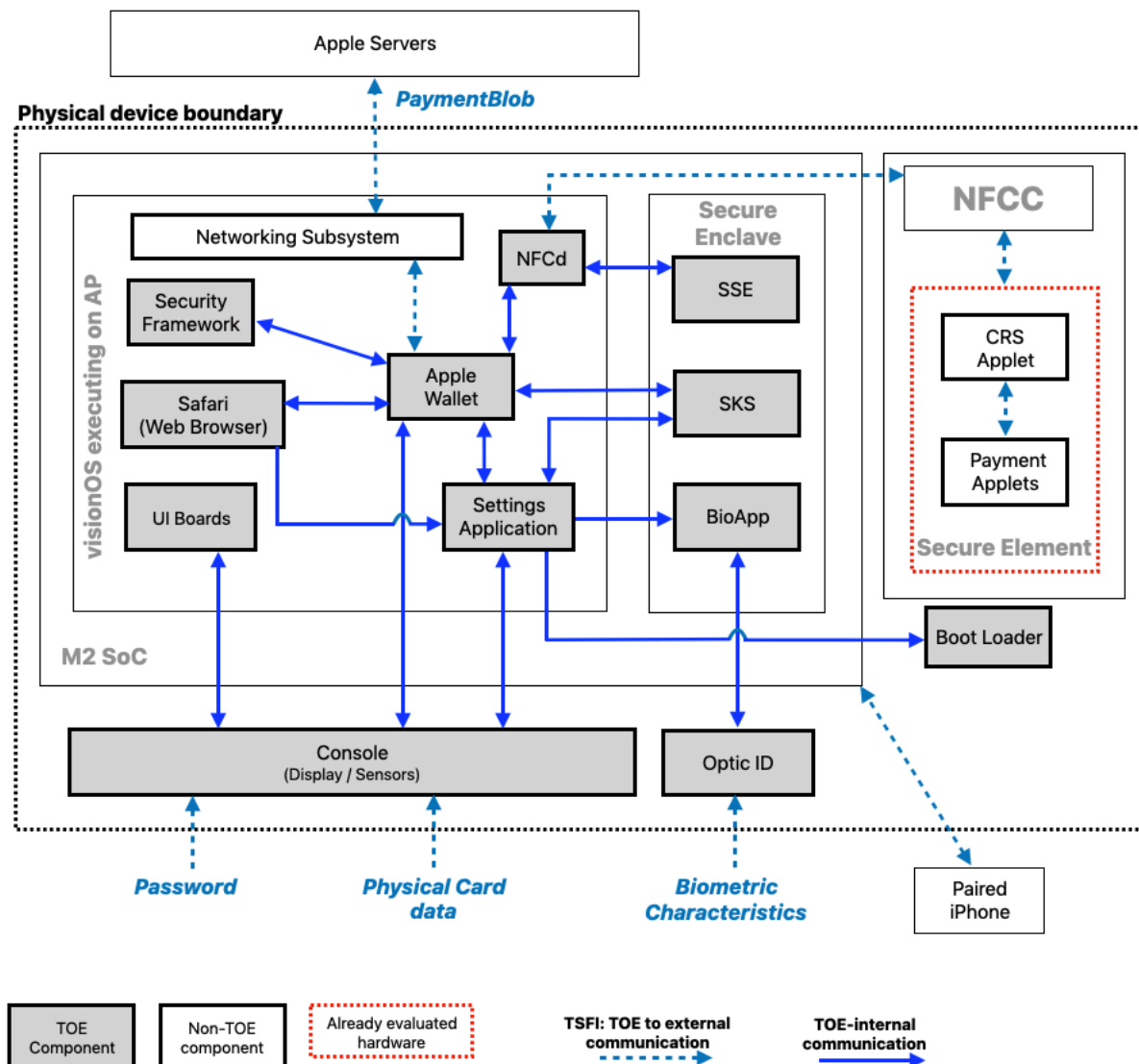


Figure 1: TOE Components and subsystems

## 2.4.2.Subsystems of the TOE

This section further breaks down the TOE components, providing more detail about the subsystems of the TOE.

The subsystems of the TOE consist of:

- Secure Enclave: The software components of the TOE residing in the Secure Enclave. This subsystem includes several applications executing on the Secure Enclave operating system:
  - BioApp is an application which provides functionality for processing biometric data and generating biometric templates
  - The SKS (Secure Key Store) is a hardware cryptographic module. The module is embedded inside the Secure Enclave and packaged within the Application Processor
  - The SSE (Secure Enclave-Secure Element) manages the pairing between the Secure Enclave and the Secure Element, allowing the Secure Element to process only genuine and authorized Apple Pay transactions. The SSE application maintains sensitive pairing material, allowing Secure Element and Secure Enclave to perform a mutual authentication before exchanging data
- Apple Wallet: The Wallet app subsystem is an application executing as part of visionOS that handles the enrollment of payment applications and governs the payment operation.
- visionOS components executing on Application Processor (AP):
  - UI Boards: The component of visionOS that handles I/O with the console, and thereby provides the functionality for the visionOS user interface
  - NFCd: This daemon facilitates the communication between Apple Wallet and the Secure Element
  - Safari browser: Web browser included with the OS. Provides a web interface to conduct payment transactions
  - Security Framework: This is an API<sup>2</sup> provided by the OS to provide cryptographic support that can be used to protect information, establish trust, and control access to software
  - Settings application: This application allows the user to modify various system settings
- Device components:
  - Optic ID: This is the hardware component and associated drivers that allow iris data to be captured and passed to BioApp to allow for enrollment and matching
  - Boot-loader: This subsystem consists of code that is executed during the boot sequence of the device. The boot-loader is responsible for ensuring that the device boots using software with assured integrity and authenticity
  - Console: This is the hardware and associated drivers that handles user input via the sensors and displays output to the user.

All other device hardware and visionOS components are outside of the TOE, including the Secure Element together with the NFCC hardware, and the XNU visionOS kernel. The visionOS subsystem components are individual applications.

---

<sup>2</sup> Refer to <https://developer.apple.com/documentation/security/>

### 2.4.3.TOE Lifecycle

The TOE lifecycle phases are as follows:

Lifecycle Phases			
<b>Design</b>	HW/FW design	SW design	Secure Element Applet design
<b>Fabrication</b>	HW fabrication	SW implementation	Applet development
<b>Integration</b>	Device integration <i>Assembly, Trust provisioning, FW integration, SW and applet loading</i>		
<b>Device Issuance</b>	Device delivery to User		
<b>Initialization</b>	User account creation Account setup: iCloud, Apple Account		
<b>Enrollment/ Provisioning</b>	User Authentication setup <i>Passcode setup, biometrics enrollment</i>		Apple Pay provisioning
<b>Usage</b>	Device Usage <i>Device unlock, User Authentication, visionOS use, (optional) visionOS update</i>		Apple Pay transaction
<b>Termination</b>	Physical destruction	visionOS reset	Apple Pay termination

The Design, Fabrication, and Integration phases are entirely within the control of Apple Inc.

The Device Issuance phase is the physical delivery of the device to the User. This can be directly, in the case of an individual, or through a third party or an entity that is responsible for providing the device to the User.

Apple's model of the Initialization phase requires that the device is claimed by the User by associating it with the User's iCloud account and Apple Account. Before that point, Strong User Authentication and associated TSFs are not relevant, and Apple Pay is not accessible. Apple Pay and Apple Cash services require that a valid iCloud account and user authentication credentials are set up (passcode and optionally biometrics).

The Usage phase describes the period when the Apple Pay service is activated and used by the associated User.

The Termination phase describes deactivation of the Apple Pay service for the User and may involve physical destruction of the device as well as a complete reset of visionOS or Apple Pay service termination by the User.

When the device is received, the model of the device should be verified against those listed in Section 2.2. Once authenticated to the device the information is available to Users in Settings » General » About. The part number is displayed next to "Model Number". To see the model number, tap the part number.

## 2.4.4. TOE security features

The logical security features of the TOE are summarized as follows:

- User authentication and management
- Secure channel between the Secure Enclave and the Biometric sensor
- Secure channel between the Secure Enclave and the Secure Element
- Secure channel between the Secure Enclave and the iPhone
- Card Data management
- Apple Pay payment transaction processing and management
- Operating System update
- iCloud logout and device reset

## 2.5. Description of the Apple Pay Service

This section contains a generic description of the Apple Pay service in general, which includes the TOE as well as the TOE environment and non-TOE hardware, software, and services.

### 2.5.1. Card provisioning

When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, Apple securely sends the card information, along with other information about the user's account and device, to the card issuer or the card issuer's authorized service provider (usually the payment network). Using this information, the card issuer (or its service provider) determines whether to approve the user's request to add the card to Apple Wallet.

As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or payment network :

- Required Fields
- Check Card
- Link and Provision

The card issuer or payment network uses these calls to enable the card issuer to verify, approve, and add cards to Apple Wallet. The confidentiality and integrity of these client server sessions are protected using TLS 1.2 or later.

Full card numbers are not stored on the device or on Apple Pay servers. Instead, a unique Device Account Number is created by the card issuer, sent encrypted to Apple, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple cannot access it. The Device Account Number is unique and different from most credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is isolated from the TOE, is never stored on Apple Pay servers, and never backed up to iCloud.

When a user provisions an eligible payment card, the user can push provision the card to other Apple Pay-capable devices on the same iCloud account using the Multi-device provisioning feature. Nothing

is copied from the original device; the other devices provision using the same flow they would use during device setup.

#### 2.5.1.1.Adding credit or debit cards manually

To add a card manually, the name, card number, expiration date, and card verification value (CVV) are used to facilitate the provisioning process. From within Setup Assistant, Settings, or Apple Wallet, users can enter the required information by typing it. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are then encrypted and sent to the Apple Pay server for routing to the card issuer or payment network.

If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the issuer's terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process.

#### 2.5.1.2.Adding credit or debit cards from an iTunes Store account

For a credit or debit card on file with iTunes, the user may be required to reenter their Apple Account password. The card number is retrieved from iTunes and the Check Card process is initiated. If the card is eligible for Apple Pay, the Apple Wallet application downloads and displays terms and conditions of the card issuer, then sends along the terms and conditions ID and the card security code to the Link and Provision process. Additional verification may occur for iTunes account cards on file.

#### 2.5.1.3.Adding credit or debit cards from a card issuer's app

When the app is registered for use with Apple Pay, keys are established for the app and for the card issuer's server. These keys are used to encrypt the card information that is sent to the card issuer. This is designed to prevent the information from being read by the Apple device. The provisioning flow is similar to that used for manually added cards, as described previously, except one-time passwords are used in lieu of the CVV.

#### 2.5.1.4.Adding credit or debit cards from a card issuer's website

Some card issuers provide the ability to initiate the card provisioning process for Apple Wallet directly from their websites. In this case, the user initiates the task by selecting a card to provision on the card issuer's website. The user is then redirected to a self-contained Apple sign-in experience (contained within Apple's domain) and is asked to sign in with their Apple Account. Upon successfully signing in, the user then chooses one or more devices to provision the card to and is required to confirm the provisioning result on each respective target device.

#### 2.5.1.5.Additional verification

A card issuer can decide whether a credit or debit card requires additional verification. Depending on what is offered by the card issuer, the user may be able to choose between different options for additional verification, such as a text message, email, a customer service call, or a method in the app of an approved card issuer to complete the verification. For text messages or email, the user is presented an option to select from contact information the issuer already holds on file. A code is sent, which must be entered into Apple Wallet, Settings. For customer service or verification using an app, the issuer performs their own communication process.

## 2.5.2.Payment authorization with Apple Pay

For devices having a Secure Element, a payment can be made only after it receives authorization from the Secure Enclave. This involves verifying that the user has confirmed their intent to pay and that the user has authenticated themselves with Optic ID or the device passcode. Optic ID, if available, is the default method, but the passcode can be used at any time. A passcode is automatically offered after two unsuccessful attempts to match an iris; after five unsuccessful attempts, the passcode is required. A passcode is also required when Optic ID is not configured or not enabled for Apple Pay.

### 2.5.2.1.Using a shared pairing key

Communication between the Secure Enclave and the Secure Element takes place over a serial interface, with the Secure Element connected to the Near Field Communication (NFC) controller, which in turn is connected to the Application Processor. Though not directly connected, the Secure Enclave and the Secure Element can communicate securely using a shared pairing key that is provisioned during the manufacturing process. The encryption and authentication of the communication are based on AES, with cryptographic nonces used by both sides to protect against replay attacks. The pairing key is generated inside the Secure Enclave from its UID key and the Secure Element unique identifier. The pairing key is then securely transferred from the Secure Enclave to a hardware security module (HSM) in the factory, which has the key material required to then inject the pairing key into the Secure Element.

### 2.5.2.2.Authorizing a secure transaction

When the user authorizes a transaction, which includes a physical gesture communicated directly to the Secure Enclave, the Secure Enclave sends signed data about the type of authentication and details about the type of transaction to the Secure Element, tied to an Authorization Random (AR) value. The AR value is generated in the Secure Enclave when a user first provisions a credit card and persists while Apple Pay is enabled, protected by the Secure Enclave encryption and anti-rollback mechanism. It is securely delivered to the Secure Element by leveraging the pairing key. On receipt of a new AR value, the Secure Element marks any previously added cards as terminated.

### 2.5.2.3.Using a payment cryptogram for dynamic security

Payment transactions originating from the payment applets include a payment cryptogram along with a Device Account Number. This cryptogram, a one-time code, is computed using a transaction counter and a key. The transaction counter is incremented for each new transaction. The key is provisioned in the payment applet during personalization and is known by the payment network or the card issuer or both. Depending on the payment scheme, other data may also be used in the calculation, including:

- An Apple Pay server anti-replay value, for transactions within apps or at websites
- User verification results, such as Cardholder Verification Method (CVM) information

These security codes are provided to the payment network and to the card issuer, which allows the issuer to verify each transaction. The length of these security codes may vary based on the type of transaction.

### 2.5.3. Paying with cards using Apple Pay

Apple Pay can be used to pay for purchases within apps and at websites.

#### 2.5.3.1. Paying with cards within apps

Apple Pay can also be used to make payments in visionOS apps. When users pay within apps using Apple Pay, Apple receives the encrypted transaction information to route to the specific developer or merchant to which the user is making a payment. Before that information is sent to the developer or merchant, Apple re-encrypts it with a developer-specific key. This is to help ensure that only an authorized developer with the key-pair can decrypt the information. Apple Pay retains anonymous transaction information, such as approximate purchase amount. This information can't be tied to the user and never includes what the user is buying.

When an app initiates an Apple Pay payment transaction, the Apple Pay servers receive the encrypted transaction from the device prior to the merchant receiving it. The Apple Pay servers then re-encrypt the transaction with a merchant-specific key before relaying it to the merchant.

When an app requests a payment, it calls an API to determine whether the device supports Apple Pay and whether the user has credit or debit cards that can make payments on a payment network accepted by the merchant. The app requests any pieces of information it needs to process and fulfill the transaction, such as the billing and shipping address, and contact information. The app then asks visionOS to present the Apple Pay sheet, which requests information for the app as well as other necessary information, such as the card to use.

At this time, the app is presented with city, state, and postal code information to calculate the final shipping cost. The full set of requested information isn't provided to the app until the user authorizes the payment with Optic ID or the device passcode. After the payment is authorized, the information presented in the Apple Pay sheet is transferred to the merchant.

#### 2.5.3.2. How users authorize, and merchants verify, app payments

Users and merchants ensure secure app payments by passing information to the Apple Pay servers, the Secure Element, the device, and the app's API. First, when the user authorizes an app payment, the app obtains a cryptographic anti-replay value, or nonce, by calling the Apple Pay servers. The servers send this value and other transaction data to the Secure Element to compute a payment credential that is encrypted with an Apple key. The Secure Element then returns the encrypted payment credential to the Apple Pay servers, which decrypt the credential, verify the nonce in the credential against the nonce that the Apple Pay servers originally sent, and re-encrypt the payment credential with the merchant key associated with the Merchant ID. The Apple Pay servers then return the payment to the device, which hands it back to the app through the API. The app then passes it along to the merchant system for processing. The merchant can then decrypt the payment credential with its private key. This, together with the signature from Apple's servers, allows the merchant to verify that the transaction was intended for this particular merchant, and ensures dynamic linking of the transaction with its amount and the payee.

The APIs require [a Merchant ID Entitlement](#) that specifies the supported Merchant IDs. An app can also include additional data (such as an order number or customer identity) to send to the Secure Element to be signed, ensuring that the transaction cannot be diverted to a different customer. This is accomplished by the app developer, who can specify applicationData on the PKPaymentRequest<sup>3</sup>. A hash of this data

---

<sup>3</sup> or PKDisbursementRequest in case of Transfer funds with Apple Pay



is included in the encrypted payment data. The merchant is then responsible for verifying that their `applicationData` hash matches what's included in the payment data.

In order to process payments, the merchant takes the following steps:

- Send the payment information to their server, along with the other information needed to process the order
- Verify the hashes and signature of the payment data
- Decrypt the encrypted payment data, and confirm the validity of the `transactionId`, `currencyCode`, `transactionAmount`, and `applicationData` fields
- Submit the payment data to the payment processing network and the order to their order-tracking system

### 2.5.3.3. Paying with cards at websites

Apple Pay can be used to make payments at websites on the device. Apple Pay on the web also requires that all participating websites register with Apple. After the domain is registered, domain name validation is performed only after Apple issues a TLS client certificate. Websites supporting Apple Pay are required to serve their content over HTTPS. For each payment transaction, websites need to obtain a secure and unique merchant session with an Apple server using the Apple-issued TLS client certificate. Merchant session data is signed by Apple. After a merchant session signature is verified, a website may query whether the user has an Apple Pay-capable device and whether they have a credit, debit, or prepaid card activated on the device. No other details are shared. If the user doesn't want to share this information, they can disable Apple Pay queries in Safari privacy settings.

If the website is using the latest version of the Apple Pay JS SDK, then Apple Pay transactions can also be started using any third-party web browser on any operating system and be completed on an Apple Pay-enabled iPhone or iPad with iOS 18, iPadOS 18, or later. For this to occur, a code must be scanned using the device's camera to establish a connection with the website. When the website presents this code, a secure WebSocket connection is made between the website and Apple's servers. Upon scanning this code, an additional separate secure WebSocket connection is made between the Apple Pay-enabled device and Apple's servers. This completes the bi-directional connection required between the website and Apple Pay-enabled device, using Apple's servers as a relay. Any communication made between these two parties then follows the usual Apple Pay on the web process.

After a merchant session is validated, all privacy and security measures are the same as when a user pays within an app.

### 2.5.3.4. Automatic payments and Merchant Tokens

Apps and websites that offer Apple Pay can take advantage of Apple Pay merchant tokens that enable secure payments consistently across a user's Apple devices. The Apple Pay payment sheet also optimizes preauthorized payment experiences. Transaction types in the Apple Pay API allow app and website developers to fine-tune the payment sheet experience for subscriptions, recurring bills, installment payments, and automatic reloads of card balances.

Merchant tokens are not device-specific, and therefore allow for continuity of recurring payments if the user removes a payment card from the device.



### 2.5.3.5. Payments to multiple merchants

Apple Pay includes the ability to specify purchase amounts for multiple merchants within a single Apple Pay payment sheet. This allows the flexibility to let customers make a bundled purchase, such as a travel package with flight, rental car, and hotel, then send payments to individual merchants.

### 2.5.4. Transfer funds with Apple Pay

Users can initiate a transfer of funds from an account to a card in Wallet. The user is not required to manually enter card details and can instead select the destination of funds directly on the payment sheet, with a concise view of any transfer fees set by the merchant. Once the user securely authenticates the transfer, an encrypted payload is generated and returned to the app, ready for processing with the payment provider. Once the transfer has been processed, the app will then return the result to Apple Pay. This uses the same secure and private Apple Pay infrastructure as payments. Transfer funds with Apple Pay is available in apps, and starting from visionOS 2.0 or later, is also available on the web.

### 2.5.5. Rendering cards unusable with Apple Pay

Credit, debit, and prepaid cards added to the Secure Element can only be used if the Secure Element is presented with authorization using the same pairing key and Authorization Random (AR) value from when the card was added. On receipt of a new AR value, the Secure Element marks any previously added cards as terminated. This allows the operating system to instruct the Secure Enclave to render cards unusable by marking its copy of the AR as invalid under the following scenarios:

- The passcode is disabled
- The user signs out of iCloud
- The user selects Erase All Content and Settings
- The device is restored from Recovery Mode

When a user erases the entire device—using Erase All Content and Settings, or restoring their device—that device instructs the Secure Element to mark all cards as terminated. This has the effect of immediately changing the cards to an unusable state until the Apple Pay servers can be contacted to fully erase the cards from the Secure Element. Independently, the Secure Enclave marks the Authorization Random as invalid so that further payment authorizations for previously enrolled cards are not possible. When the device is online, it attempts to contact the Apple Pay servers to help ensure that all cards in the Secure Element are erased.

#### 2.5.5.1. Suspending, removing, and erasing cards

Users can suspend Apple Pay, or remove and erase their cards from the device using the following methods:

- Apple Wallet
- Remove device from Apple Account
- Remove device from icloud.com
- Delete Apple Account from the Apple [Data and Privacy page](#)

When a user suspends or removes cards from Apple Pay, the ability to make payments using those cards is suspended or revoked by the card issuer or respective payment network, even if the device is offline

and not connected to a Wi-Fi or cellular network. Users can also contact their card issuer to suspend or remove cards from Apple Pay.

## 2.5.6.Apple Card

On supported devices a user can securely apply for an Apple Card.

### 2.5.6.1.Apple Card application

On devices with iOS 12.4 or later, iPadOS 13.1 or later, macOS 10.14.6 or later, watchOS 5.3 or later, and visionOS 1.0 or later, Apple Card can be used with Apple Pay to make payments in apps and on the web. Apple Card is currently only available for qualifying applicants in the United States.

To apply for Apple Card, the user must be signed into their iCloud account on an Apple Pay-compatible device and have two-factor authentication set up on the iCloud account, or they can apply at <https://apply.applecard.apple/> after signing in with their Apple Account. When the application is approved, Apple Card is available in the Apple Wallet app or within Settings > Wallet & Apple Pay across any of the eligible devices the user has signed in with their Apple Account.

When a user applies for Apple Card, user identity information is securely verified by Apple's identity provider partners and then shared with Goldman Sachs Bank USA for the purposes of identity and credit evaluation.

Information such as the social security number or ID document image provided during the application is securely transmitted to Apple's identity provider partners and/or Goldman Sachs Bank USA encrypted with their respective keys. Apple can't decrypt this data.

The income information provided during the application, and the bank account information used for bill payments, are securely transmitted to Goldman Sachs Bank USA encrypted with their key. The bank account information is saved in Keychain. Apple can't decrypt this data.

When adding Apple Card to the Apple Wallet app, the same information as when a user adds a credit or debit card may be shared with the Apple partner bank, Goldman Sachs Bank USA, and with Apple Payments Inc. This information is used only for troubleshooting, fraud prevention, and regulatory purposes.

In iOS 14.6 or later, iPadOS 14.6 or later, and watchOS 7.5 or later, the organizer of an iCloud family with an Apple Card can share their card with their iCloud Family members over the age of 13. User authentication is required to confirm the invitation. Apple Wallet uses a key in the Secure Enclave to compute a signature that binds the owner and the invitee. That signature is validated on Apple servers.

Optionally, the organizer can set a transaction limit for the participants. Participant cards can also be locked to pause their spending at any time through the Apple Wallet app. When a co-owner or participant over the age of 18 accepts the invitation and applies, they go through the same application process in the Apple Wallet app as defined above.

### 2.5.6.2.Apple Card usage

A physical card can be ordered from Apple Card in Apple Wallet. After the user receives the physical card, it's activated using the NFC tag that's in the bifold envelope of the physical card. The tag is unique per card and can't be used to activate another user's card. Alternatively, the card can be manually activated in Apple Wallet settings. Additionally, the user can also choose to lock or unlock the physical card at any time from Apple Wallet.

### 2.5.6.3.Apple Card payments and Apple Wallet pass details

Payments due on the Apple Card account can be made from a web browser or the Apple Wallet app in visionOS with Apple Cash and a bank account. Bill payments can be scheduled as recurring or as a one-time payment at a specific date with Apple Cash and a bank account. When a user makes a payment, a call is made to the Apple Pay servers to obtain a cryptographic nonce similar to Apple Cash. The nonce, along with the payment setup details, is passed to the Secure Element to compute a signature. The signature is then returned to the Apple Pay servers. The authentication, integrity, and correctness of the payment are verified through the signature and the nonce by Apple Pay servers, and the order is passed on to Goldman Sachs Bank USA for processing.

The Apple Card number is retrieved by Apple Wallet by presenting a certificate. The Apple Pay server validates the certificate to confirm the key was generated in the Secure Enclave. It then uses this key to encrypt the Apple Card number before returning it to Apple Wallet, so that only the iPhone that requested the Apple Card number can decrypt it. After decryption, the Apple Card number is saved in iCloud Key-chain.

Displaying the Apple Card number details in the pass using the Apple Wallet app requires user authentication with a Biometric or a passcode. It can be replaced by the user in the card information section and disables the previous one.

### 2.5.6.4.Advanced Fraud Protection

The Apple Card user can enable Advanced Fraud Protection in the Apple Wallet app. When enabled, the Card Security Code refreshes every few days.

### 2.5.7.Apple Cash

On devices with iOS 11.2 or later, iPadOS 13.1 or later, watchOS 4.2 or later, and visionOS 1.0 or later, Apple Cash can be used to send, receive, and request money from other users. When a user receives money, it is added to an Apple Cash account that can be accessed in the Apple Wallet app or within Settings > Wallet & Apple Pay across any of the eligible devices the user has signed in with their Apple Account. Apple Cash is currently only available to users in the United States.

On devices with iOS 14 or later, iPadOS 14 or later, and watchOS 7 or later, the organizer of an iCloud family who has verified their identity with Apple Cash can enable Apple Cash for their family members under the age of 18. Optionally, the organizer can restrict the money sending capabilities of these users to family members only or contacts only. If the family member under the age of 18 goes through an Apple Account recovery, the organizer of the family must manually reenable the Apple Cash card for that user. If the family member under the age of 18 is no longer part of the iCloud family, their Apple Cash balance is automatically transferred to the organizer's account.

When the user sets up Apple Cash, the same information as when the user adds a credit or debit card may be shared with Apple's partner bank in the United States, Green Dot Bank, and with Apple Payments Inc., a wholly owned subsidiary created to protect the user's privacy by storing and processing information separately from the rest of Apple, and in a way that the rest of Apple doesn't know. This information is used only for troubleshooting, fraud prevention, and regulatory purposes.

#### 2.5.7.1.Using Apple Cash in iMessage

To use person-to-person payments and Apple Cash, a user must be signed into their iCloud account on an Apple Cash compatible device and have two-factor authentication set up on the iCloud account.

Money requests and transfers between users are initiated from within the Messages app or by asking Siri. When a user attempts to send money, iMessage displays the Apple Pay sheet. The Apple Cash balance is always used first. If necessary, additional funds are drawn from a second credit or debit card the user has added to the Apple Wallet app.

### 2.5.7.2. Using Apple Cash in apps and on the web

The Apple Cash card in the Apple Wallet app can be used with Apple Pay to make payments in apps and on the web. Money in the Apple Cash account can also be transferred to a bank account. In addition to money being received from another user, money can be added to the Apple Cash account from a debit or prepaid card in the Apple Wallet app.

Apple Payments Inc. stores, and may use, the user's transaction data for troubleshooting, fraud prevention, and regulatory purposes once a transaction is completed. The rest of Apple doesn't know who the user sent money to, received money from, or where the user made a purchase with their Apple Cash card.

When the user sends money with Apple Pay, adds money to an Apple Cash account, or transfers money to a bank account, a call is made to the Apple Pay servers to obtain a cryptographic nonce, which is similar to the value returned for Apple Pay within apps. The nonce, along with other transaction data, is passed to the Secure Element to compute a payment signature. The signature is returned to the Apple Pay servers. The authentication, integrity, and correctness of the transaction is verified through the payment signature and the nonce by Apple Pay servers. Money transfer is then initiated, and the user is notified of a completed transaction.

If the transaction involves:

- A debit card for adding money to Apple Cash
- Providing supplemental money if the Apple Cash balance is insufficient

An encrypted payment credential is also produced and sent to Apple Pay servers, similar to how Apple Pay works within apps and websites.

After the balance of the Apple Cash account exceeds a certain amount or if unusual activity is detected, the user is prompted to verify their identity. Information provided to verify the user's identity - such as social security number or answers to questions (for example, to confirm a street name the user lived on previously) - is securely transmitted to the Apple partner and encrypted using their key. Apple can't decrypt this data. The user is prompted to verify their identity again if they perform an Apple Account recovery, before regaining access to their Apple Cash balance.

## 2.6. TOE Use Cases

The TOE covers the following use cases:

Use Case	Description
<b>UC.Device_Usage</b>	<u>Device usage</u> The User can manage the device's authentication credentials, including enrolling new biometric templates, updating biometric templates, deleting biometric templates and changing the passcode.

Use Case	Description
<b>UC.OS_Update</b>	<u>Device Software Update</u> The User can perform an update of the software in the device to a new version.  This use case requires that the User verifies the device's passcode.  This use case ensures preservation of the User settings on the device: <ul style="list-style-type: none"><li>• No change to the User's authentication credentials (passcode or any biometrics)</li><li>• No change to the User's data within the Secure Element unless specified by the data's issuer</li></ul>
<b>UC.Apple_Pay_Install_Init</b>	<u>Apple Pay installation and initialization</u> The User can provision a new card in Apple Wallet
<b>UC.Apple_Pay_Usage</b>	<u>Apple Pay usage</u> The User can perform Apple Pay transactions.
<b>UC.End_Of_Service</b>	<u>Termination by User</u> The User can end the Apple Pay mode of operation by performing a card removal in Apple Wallet.  The User can also end all current Apple Pay services by un-registering their iCloud account.  <u>Termination by card issuer</u> The card issuer can perform a de-registration of an Apple Pay card that was provisioned on the User's device, following a card revocation or a user account termination.
<b>UC.End_Of_Life</b>	<u>Termination of device</u> The User can clear a device from all their settings and data by performing a device full reset.  The User could also end the life of their device by physically destroying it.

## 3. Evaluation Assurance

### 3.1. Common Criteria Reference

This Security Target is based on the following Common Criteria™ (CC) publications:

Common Criteria	CC Version	Revision	Date
<b>Part 1: Introduction and general model</b>	CC:2022	R1	November 2022
<b>Part 2: Security functional requirements</b>	CC:2022	R1	November 2022
<b>Part 3: Security assurance requirements</b>	CC:2022	R1	November 2022
<b>Part 4: Framework for the specification of evaluation methods and activities</b>	CC:2022	R1	November 2022
<b>Part 5: Pre-defined packages of security requirements</b>	CC:2022	R1	November 2022

### 3.2. CC Conformance claim

This Security Target is **conformant** to CC Part 2 and CC Part 3.

### 3.3. Protection Profile Conformance claim

This Security Target does not claim any conformance to an existing Protection Profile.

### 3.4. Assurance Level

The evaluation assurance level (EAL) for this work is EAL 2 augmented with ADV\_FSP.3 and ALC\_FLR.3:

Assurance Class	
<b>ADV: Development</b>	ADV_ARC.1 Security architecture description
	<b>ADV_FSP.3 Functional specification with complete summary</b>
	ADV_TDS.1 Basic design
<b>AGD: Guidance documents</b>	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
<b>ALC: Life-cycle support</b>	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	<b>ALC_FLR.3 Systematic flaw remediation</b>
<b>ASE: Security Target evaluation</b>	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition

Assurance Class	
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

## 4. Security Problem Definition

### 4.1. Assets

The assets of the TOE are:

Asset	Sensi- tivity*	Type	Definition
<b>D.User_Passcode</b>	I, C	User	Passcode value setup by the User, used to wake up the device after power loss, unlock the device, and to authorize payments (Apple Pay transactions or Apple Cash transfers).
<b>D.User_Bio</b>	I, C	User	Biometric data for the enrolled User's biometrics, used to unlock the device and to authorize payments (Apple Pay transactions or Apple Cash transfers).
<b>D.Card_Data</b>	I, C	User, TSF	Apple Pay card data, including credit/debit card number, User's name, expiration date, CVV, and transaction data (e.g., transaction history).  Apple Cash card data, including Apple Cash card information and transfer data (e.g., transfer history).  Note: The card data is used as TSF data when the TOE sends it encrypted to the card issuer, via Apple servers, in order to generate the Device Account Number stored in the Secure Element.
<b>D.User_Intent</b>	I	User	State of the device resulting from a physical interaction of the User with the TOE, characterizing the intent of the User to perform a transaction (Apple Pay transactions or Apple Cash transfers)
<b>D.Payment_Data</b>	I	User	Apple Pay/Apple Cash payment data being authorized by the User. For Apple Pay, critical elements are the amount (including the currency), the emitter, and the recipient (S.Merchant) which constitute the core of the Dynamic Linking. For Apple Cash, critical elements of transfers are the amount (including the currency), the emitter, and the recipient. Additional critical elements can be defined by Apple and the card issuer.
<b>D.OS</b>	I	TSF	OS version currently installed on the device. This asset is not the OS code itself or the version number of that code. This asset is the set of elements that compose an OS version as prepared for that device, including elements verifiable by that device during boot (for instance the sepOS), and by the User through an identified version number.
<b>D.User_Configuration</b>	I	TSF	User configuration is a representation of the user personal configuration including Apple Pay, Apple Cash, and Optic ID settings.



Asset	Sensitivity*	Type	Definition
<b>D.SEP_Configuration</b>	I	TSF	Secure Enclave configuration is a representation of the state of the Secure Enclave in the device. It comprises (but is not limited to) the Secure Enclave OS version and the state of the user authentication functions (passcode, enrolled biometrics, authenticated credentials, retry counters, and authentication-based access control settings).
<b>D.SEP_SE</b>	I, C	TSF	Secret data that allows secure communication between the Secure Enclave and the Secure Element during processing of an Apple Pay transaction or Apple Cash transfer.
<b>D.SEP_Bio</b>	I, C	TSF	Secret data that allows secure communication between the Secure Enclave and the biometric sensor during processing of biometric authentication.
<b>D.SEP_iPhone</b>	I, C	TSF	Secret data that allows secure communication between the Secure Enclave on the TOE and the Secure Enclave on the Paired iPhone, in the case the Paired iPhone is used for the "Nearby iPhone enables Optic ID" feature. The asset is also referred to in this ST as the Secure Enclave iPhone pairing secret.
<b>D.EnableOpticID_Secret</b>	I, C	TSF	Secret data that is shared by the Secure Enclave on the TOE with the Paired iPhone Secure Enclave to enable Optic ID. It is released by the Paired iPhone to enable the use of Optic ID to unlock the TOE after turning on or restarting the TOE. This asset is created by the TOE when the "Nearby iPhone enables Optic ID" feature is enabled by the User, and does not exist if there is no Paired iPhone or if this feature is disabled. The asset is also referred to in this ST as the Optic ID Enablement Secret.

\*: I = Integrity, C = Confidentiality

## 4.2. Subjects

The subjects of this Security Target are:

Subject	Definition
<b>S.User</b>	User of Apple Pay/Apple Cash on the device, able to: <ul style="list-style-type: none"> <li>Authenticate on the device (biometrics or passcode)</li> <li>Manage authentication credentials (biometrics or passcode)</li> <li>Manage device configuration (OS version, iCloud account)</li> <li>Provision/enroll cards</li> <li>Authorize Apple Pay transactions/Apple Cash transfers by providing consent for the transaction to proceed (biometrics/passcode and user intent)</li> <li>Cancel the Apple Pay/Apple Cash service</li> </ul>

Subject	Definition
<b>S.Apple_Servers</b>	Apple servers in charge of: <ul style="list-style-type: none"><li>• Management of S.User iCloud account</li><li>• Management of S.User provisioning/enrollment in Apple Pay/Apple Cash</li><li>• Management of OS releases, including Apple Wallet app</li><li>• Device's interface for processing Apple Pay transactions/ Apple Cash transfers (contact S.Issuer)</li></ul>
<b>S.Issuer</b>	The card issuer (or its service provider) is the third party in charge of: <ul style="list-style-type: none"><li>• Management of S.User data for Apple Pay/Apple Cash services</li><li>• Processing Apple Pay transactions/Apple Cash transfers</li></ul>
<b>S.Merchant</b>	The merchant is the third-party accepting payment through an Apple Pay transaction.
<b>S.SE</b>	Certified Secure Element of the device including the TOE.
<b>S.iPhone</b>	iPhone belonging to S.User, paired with the TOE (if the "Nearby iPhone Enables Optic ID" feature is enabled).

### 4.3. Assumptions

The assumptions for this Security Target are the following:

Assumption	Definition
<b>A.DEVICE_AUTH</b>	The User of the device ensures that all the Apple Pay and Apple Cash activities that are performed on the device have been authorized by the User. All authentication credentials (Biometrics or passcode) for the device that are enabled for use with Apple Pay/Apple Cash are owned and protected by the User of the device.
<b>A.PERSO</b>	The Apple Pay and Apple Cash card issuers guarantee the correctness of the card data input in the device during provisioning/enrollment: Data shall uniquely identify a financial payment means and be linked to the account owned by the identified user.
<b>A.IPHONE_USER</b>	If the User optionally pairs an iPhone with their TOE device, they own it and ensure the confidentiality of its authentication credentials.

### 4.4. Threat Agents

The threat agents of this TOE are the following:

Threat Agent	Definition
<b>S.Attacker</b>	A threat agent trying to interact with the Apple Pay and Apple Cash system fraudulently, trying to modify the configuration and data of genuine Users' devices or forging data on their own device.

## 4.5. Threats

The threats to assets of this TOE are the following:

Threat	Name	Definition	Assets
<b>T.CORRUPT</b>	Corrupted Transaction or Transfer	An attacker attempts to corrupt an Apple Pay transaction or an Apple Cash transfer. To gain from the attack, the attacker could be the emitter of the transaction or transfer, and attempt to reduce what it intends to pay (debit amount from attacker's account) from what it was supposed to pay (credit amount request or transfer amount agreed between attacker and victim). The attacker could also attempt to corrupt a payment when it is the recipient, and increase what it supposed to receive (credit transaction amount) from what it was supposed to receive (debit amount agreed). The attacker could also attempt to modify the recipient of a credit transaction by changing the payee in an Apple Pay transaction or changing the recipient of an Apple Cash transfer.	D.Payment_Data D.User_Configuration D.OS
<b>T.PHYSICAL</b>	Physical	The loss or theft of the device may give rise to loss of confidentiality of User data including credentials and TSF data. These physical access threats may involve attacks which attempt to access the device through external hardware ports, through its user interface, and also through direct and possibly destructive access to its storage media. The goal of such attacks is to access Apple Pay or Apple Cash data from a lost or stolen device which is not expected to return to its User. <i>Note: Defending against device re-use after physical compromise is out of scope.</i>	D.User_Passcode D.User_Bio D.Card_Data D.EnableOpticID_Secret* D.SEP_iPhone*
<b>T.RECOVER</b>	Card Recovery	An attacker attempts to recover Apple Pay or Apple Cash card data from an erased or blocked device and use it to perform a financial transaction or transfer. The attacker will target potential breaches in the process of Apple Pay cancellation, Apple Pay card revocation, Apple Cash disenrollment, Apple Cash card revocation, or visionOS erase all content and settings.	D.User_Configuration D.Card_Data D.OS
<b>T.REPLAY</b>	Replay	An attacker attempts to replay an Apple Pay transaction or an Apple Cash transfer.	D.Payment_Data
<b>T.SILENT</b>	Silent Transaction	An attacker attempts to modify the behavior of the device, in order to perform silent Apple Pay transactions or Apple Cash transfers for some benefit. The attacker would have to perform the attack without knowledge of the device's rightful owner who will be the victim of the attack.	D.User_Intent D.User_Configuration D.SEP_Configuration D.SEP_SE D.OS

Threat	Name	Definition	Assets
<b>T.SKIMMING</b>	Authenticat- ion Bypass	An attacker attempts to perform a payment with Apple Pay or Apple Cash, bypassing the required authentication step (biometrics data verification or passcode verification).	D.User_Intent D.Payment_Data D.SEP_Configuration D.User_Configuration D.OS
<b>T.USURP</b>	Card Own- ership Usurpation	An attacker could attempt to authenticate on a de- vice, with a goal of using any provisioned cards on that device. The attacker could focus on the card data during Apple Pay provisioning or Apple Cash enrollment.	D.User_Bio D.User_Passcode D.User_Configuration D.SEP_Bio D.Card_Data D.OS D.EnableOpticID_Se- cret* D.SEP_iPhone*

\* Partial threat: On its own, Enabling Optic ID for device unlock after power on or reset does not give the attacker access to the TOE or its assets.

Assets & Threats mapping table:

Asset - Property - I = Integrity C = Confidentiality		T.CORRUPT	T.PHYSICAL	T.RECOVER	T.REPLAY	T.SKIMMING	T.SILENT	T.USURP
D.EnableOpticID_Secret	I,C		X					X
D.User_Bio	I,C		X					X
D.User_Passcode	I,C		X					X
D.User_Intent	I					X	X	
D.Payment_Data	I	X			X	X		
D.Card_Data	I,C		X	X				X
D.OS	I	X		X		X	X	X
D.User_Configuration	I	X		X		X	X	X
D.SEP_Configuration	I					X	X	
D.SEP_iPhone	I,C		X					X
D.SEP_SE	I,C						X	
D.SEP_Bio	I,C							X

## 4.6. Organizational Security Policies

The organizations associated with the Apple Pay service shall comply with the following Organizational Security Policies as security rules, procedures, practices, or guidelines imposed by an organization upon its operations:

OSP	Definition
<b>P.UPDATE</b>	Apple ensures that only an authenticated User ( <i>S.User</i> ) can update their device's operating system to a newly released visionOS. Apple also informs the Apple Pay and Apple Cash card issuers and PNOs of new applicable features of new releases.
<b>P.DYN_LINK</b>	Apple enables the enforcement of Dynamic Linking for e-Commerce payments using Apple Pay or Apple Cash cards, on device side and server side. This Organizational Security Policy guarantees that Apple preserves the following properties from design to feature release for Apple Pay and Apple Cash e-commerce payments: <ul style="list-style-type: none"><li>(a) The payer is made aware of the amount of the payment transaction and of the payee.</li><li>(b) The authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction.</li><li>(c) The authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer.</li><li>(d) Any change to the amount or the payee results in the invalidation of the authentication code.</li></ul>
<b>P.IPHONE</b>	The TOE allows the User to use the "Nearby iPhone enables Optic ID" feature through a secure channel when an optional iPhone is paired with the TOE device. When this feature is enabled, and the user is signed in to their iPhone running iOS 17.1 or later and their TOE device with the same Apple Account, having their iPhone nearby can enable the use of Optic ID to unlock the TOE device when it is turned on or restarted. The user can use this feature if their iPhone is nearby and has been unlocked in the past hour.

## 5. Security Objectives

### 5.1. Security Objectives for the TOE

Security Objectives	Definition
<b>OT.User_Auth</b>	The TOE enforces the following authentication policy: <ul style="list-style-type: none"><li>• Passcode only:<ul style="list-style-type: none"><li>- Add, update, or delete Biometrics</li><li>- Update passcode</li><li>- Modify authentication policy</li><li>- Update the OS to a new version signed by Apple</li></ul></li><li>• Passcode or biometric (if enrolled)<ul style="list-style-type: none"><li>- Unlock of the device</li><li>- Payment confirmation</li></ul></li></ul>
<b>OT.Card_Data</b>	The TOE enforces that sensitive card data: <ul style="list-style-type: none"><li>• Is encrypted before being sent to the Apple server</li><li>• Is not accessible after sent to the Apple server</li></ul>
<b>OT.Passcode_Delete</b>	The TOE enforces that removing the passcode: <ul style="list-style-type: none"><li>• Disables biometric authentication</li><li>• Disables Apple Pay/Cash</li></ul>
<b>OT.Card_Delete</b>	The TOE securely triggers the deletion of each individual Apple Pay/Apple Cash card when: <ul style="list-style-type: none"><li>• A card is removed from Apple Wallet</li><li>• The TOE handles the revocation of a card by its issuer</li><li>• The use of Apple Pay is disabled (from iCloud, the Settings or passcode removal)</li><li>• The iCloud account is no longer associated with the device</li></ul> <p>When a card is removed, the TOE also instructs the Secure Element to mark it as terminated.</p>
<b>OT.Auth_SE</b>	The TOE provides the Secure Element with passcode/biometric user authentication features for Apple Pay/Apple Cash payment/transfer approval.
<b>OT.Payment</b>	For eCommerce transactions and Apple Cash transfers, the TOE enforces that transaction details are displayed to the User (including the card to be used from Apple Wallet, the amount, and the payee) before the User shows their intent to pay and authenticates for payment validation. The TOE ensures that these details cannot be corrupted between the payment validation and the moment when details are sent to the Secure Element.  The TOE also requests explicit intent from the User for Apple Pay transactions and Apple Cash transfers.
<b>OT.Bio_Delete</b>	TOE Biometrics delete is a secure erase of the enrolled biometric data.
<b>OT.Device_Reset</b>	TOE securely deletes all User data when the User launches an "Erase All Content and Settings" on the OS or a device erase from iCloud. This also initiates the disabling of Apple Pay/Apple Cash and plans the destruction of Apple Pay/Apple Cash cards that will be effective when the device is restored.

Security Objectives	Definition
<b>OT.Anti_Replay</b>	The TOE ensures that each payment processed by an Apple Pay/Apple Cash card holds the unique identifier.
<b>OT.OS_Update</b>	TOE enforces security measures ensuring preservation of User data when an OS update is installed in the TOE. This objective protects the user authentication credentials (Biometrics and passcode), the Apple Pay card data, the Apple Cash card, and more.
<b>OT.iPhone</b>	The TOE can enforce secured communication with an optional paired iPhone.

## 5.2. Security Objectives for the environment

Environment Security Objectives	Definition
<b>OE.Card_Data</b>	<p>The card 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 during enrolment.</p> <p>The Secure Element is responsible for securing the card validation exchanges with the card issuer's TSM and for ensuring confidentiality and integrity of each card's sensitive data during storage and use.</p>
<b>OE.Perso</b>	The card 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 card issuer also ensures the robustness of the personalization data, to prevent attacks like forgery, counterfeit, or corruption.
<b>OE.Card_Delete</b>	<p>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 Erase All Content and Settings. The card 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 card issuer or the corresponding TSP).</p> <p>The Secure Element is responsible for securely deleting the stored card sensitive data (private/secret).</p>
<b>OE.Anti_Replay</b>	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.
<b>OE.Transaction_Verification</b>	<p>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). The cryptogram validation result allows the card issuer to approve or reject the transaction. The payment is invalidated if this verification fails.</p> <p>For Apple Cash, the Apple Cash 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 device completes transfer processing). The modifications that the server is able to detect cover, but are not limited to, the amount and the recipient.</p>
<b>OE.Dynamic_Linking</b>	For eCommerce transactions, the Apple Pay server preserves and card issuer server verifies the cryptographic based dynamic linking of the transaction data (including amount and payee). The payment is invalidated if this verification fails.

Environment Security Objectives	Definition
<b>OE.Statement</b>	For Apple Pay, the 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 card issuer ensures that the ledger associated to an Apple Cash account (list of transfers including completed, canceled, and pending) is fully accurate.
<b>OE.Genuine_Wallet</b>	The Apple Wallet application is provided and signed by Apple.
<b>OE.iPhone</b>	The S.iPhone is responsible for ensuring the confidentiality of the unlock secret provided by the Vision Pro during all its lifetime: from inception at enabling of the “Nearby iPhone enables Optic ID” feature, during its storage, during its release for enabling Optic ID, and when it is deleted when the feature is disabled.  The S.iPhone is responsible for ensuring that it is protected by a passcode.
<b>OE.User</b>	The User is responsible for ensuring that: <ul style="list-style-type: none"> <li>• They authorize all the Apple Pay/Cash activities that are performed on the device</li> <li>• The passcode is robust and protected</li> <li>• Only their own biometrics credentials are enrolled (they do not enroll biometrics of someone else)</li> <li>• Only their own iPhone is paired with the TOE and the paired iPhone is protected. This includes abiding by the iOS Software License Agreement and protecting the confidentiality of the paired iPhone’s passcode</li> </ul>

### 5.3. Rationale of the Security objectives for the security problem definition

The following table details the rationale for each element of the security problem definition. For all the objectives for the TOE, OT.OS\_Update also ensures the authentication configuration is preserved during the OS update.

Element	Rationale
<b>A.DEVICE_AUTH</b>	OE.User and OE.iPhone cover A.DEVICE_AUTH ensuring the User owns and protects all the authentication credentials and the User authorizes the Apple Pay and Apple Cash activities that are performed on the device.
<b>A.PERSO</b>	OE.Perso covers A.PERSO ensuring the provisioning process verifies the ownership of the provisioned cards.
<b>A.IPHONE_USER</b>	OE.User and OE.iPhone cover A.IPHONE_USER ensuring the User of the device owns and protects their iPhone and related credentials.
<b>T.SKIMMING</b>	OT.User_Auth, OT.Auth_SE and OT.Payment ensure that an Apple Pay transaction or an Apple Cash transfer is always authenticated and authorized by the User. OT.User_Auth and OE.Genuine_Wallet ensure that the Apple release of a new OS or Apple Wallet app implementing the authentication functions and payment functions are controlled, and that it preserves the confidentiality and integrity of the authentication and payment data. OT.Passcode_Delete ensures that if the passcode is turned off, the Apple Pay and Biometric authentication are not available anymore.



Element	Rationale
<b>T.USURP</b>	<p>OT.Card_Data, OT.OS_Update and OE.Card_Data ensure that the Apple Pay/Apple Cash card data are kept confidential and not altered from an attacker during storage and use in the Secure Element.</p> <p>OT.User_Auth, OT.Auth_SE and OT.Payment prevent the attacker from attempting to perform Apple Pay transactions or Apple Cash transfers, enforcing user authentication with set credentials (which are not known or owned by the attacker according to OE.User), and preventing the attacker from replacing a User's passcode or biometrics with their own.</p> <p>OT.User_Auth and OE.Genuine_Wallet additionally ensure that the installation of a new Apple released OS or Apple Wallet app preserves the confidentiality and integrity of the payment data.</p> <p>OT.Passcode_Delete ensures that if passcode login is disabled, the Apple Pay and Biometric authentication are not available anymore.</p>
<b>T.RECOVER</b>	<p>OT.Bio_Delete ensures that a removed passcode or biometric credential cannot be recovered.</p> <p>OT.Card_Data, OT.OS_Update and OE.Card_Data ensure that the confidential card data is only stored by the Secure Element which protects them from disclosure.</p> <p>OT.Device_Reset covers the physical erase of the content and settings of the device where the TOE will trigger secure erase all provisioned card data. OE.Card_Delete ensures that the issuers of provisioned cards are securely removing the deleted cards from the User's account so that no transaction can further proceed.</p>
<b>T.REPLAY</b>	<p>OE.Anti_Replay and OT.Anti_Replay ensure that each Apple Pay transaction or Apple Cash transfer cannot be replayed.</p> <p>OT.User_Auth and OE.Genuine_Wallet additionally ensure that the installation of a new Apple released OS or Apple Wallet application preserves transaction replay protection.</p>
<b>T.CORRUPT</b>	<p>OT.Payment enforces the dynamic linking of the Apple Pay transaction data, ensuring that the critical content (such as emitter, recipient, amount) cannot be changed after the transaction was processed using a provisioned card. OE.Dynamic_Linking ensures that the Apple Pay server is verifying the integrity of the Apple Pay transaction data Dynamic Linking. OE.Statement provides an additional verification point for the account holder as the card issuer ensures that all processed Apple Pay transactions appear on the statement of the account associated to the card.</p> <p>OT.User_Auth and OE.Genuine_Wallet ensure that the Apple release of a new OS or Apple Wallet implementing the payment functions are controlled.</p>

Element	Rationale
<b>T.SILENT</b>	<p>OT.User_Auth and OT.Payment ensure that an Apple Pay transaction or Apple Cash transfer is always authorized by the User.</p> <p>OE.Statement ensures that the Apple Pay card issuers provide account holder verification material (in the form of transaction statements) allowing them to identify any fraudulent activity on their account. The Apple Cash card issuer ensures that the ledger associated to an Apple Cash account (list of transfers including completed/canceled/pending) is fully accurate.</p> <p>OT.User_Auth and OE.Genuine_Wallet ensure that the Apple release of a new OS or Apple Wallet implementing the authentication functions and payment functions is controlled.</p> <p>OT.Passcode_Delete ensures that if passcode is turned off, the Apple Pay and Biometric authentication are not available anymore.</p>
<b>T.PHYSICAL</b>	<p>The User credentials maintained by the TOE are secured by OT.User_Auth enforcing the secure verification process of Biometrics or passcode.</p> <p>The TOE lifecycle is secure through the management of the device within the Apple iCloud environment where the User is able to remove the device from its account (OT.Card_Delete) and reset the device's content (OT.Device_Reset). This binding ensures that the User's critical data is safe in case device is lost or stolen.</p> <p>OT.Card_Data, OT.OS_Update and OE.Card_Data ensure that the provisioned card data is kept confidential in the Secure Element and cannot be extracted.</p>
<b>P.UPDATE</b>	<p>OT.User_Auth and OE.Genuine_Wallet ensure that the Apple release of a new OS or Apple Wallet implementing the authentication functions and payment functions are controlled, and that it preserves the confidentiality and integrity of the authentication and payment data.</p>
<b>P.DYN_LINK (Dynamic Linking)</b>	<p>P.DYN_LINK is covered by OT.Payment, OT.User_Auth, OT.Anti_Replay, OE.Anti_Replay, OE.Transaction_Verification, and OE.Dynamic_Linking, which all participate in the enforcement of the Dynamic Linking requirements on e-Commerce payments. The mapping is as follows:</p> <p>(a) OT.Payment ensures that there is a step, part of the user intent confirmation phase, when the User (payer) is made aware of the amount of the payment transaction and payee.</p> <p>(b) OT.User_Auth ensures that the user authentication was performed to ensure agreement by the payer to authorize the Apple Pay transaction data (specific to the payer, amount, and payee), OT.Anti_Replay ensures that each payment is uniquely identified, and OT.Payment ensures that the payment data is integrity protected.</p> <p>(c) OE.Anti_Replay, OE.Transaction_Verification and OE.Dynamic_Linking ensure that the received Apple Pay transaction data correspond to what was agreed to by the payer: The unique identifier to prevent replay is verified, the cryptogram for the data is verified, and the dynamic linking of the user authentication and the payment data integrity is verified.</p> <p>(d) OE.Anti_Replay, OE.Transaction_Verification and OE.Dynamic_Linking ensure that any change to the amount or the payee results in the invalidation of the payment and its unique identifier so no replay is attempted.</p>
<b>P.IPHONE</b>	<p>P.IPHONE is covered by OT.User_Auth, OT.iPhone, OE.iPhone, and OE.User, which ensure that only the user's iPhone can be used for the "Nearby iPhone enables Optic ID" feature.</p>

Security Objectives mapping table:

	T.CORRUPT	T.PHYSICAL	T.RECOVER	T.REPLAY	T.SILENT	T.SKIMMING	T.USURP	P.DYN_LINK	P.UPDATE	P.IPHONE	A.PERSO	A.DEVICE_AUTH	A.IPHONE_USER
OT.Anti_Replay				x				x					
OT.Card_Data		x	x				x						
OT.Payment	x				x	x	x	x					
OT.Card_Delete		x											
OT.OS_Update		x	x				x						
OT.Auth_SE						x	x						
OT.User_Auth	x	x		x	x	x	x	x	x	x			
OT.iPhone										x			
OT.Passcode_Delete					x	x	x						
OT.Bio_Delete			x										
OT.Device_Reset		x	x										
OE.Anti_Replay				x				x					
OE.Card_Data		x	x				x						
OE.Perso											x		
OE.Dynamic_Linking	x							x					
OE.Statement	x				x								
OE.Transaction_Verification								x					
OE.iPhone										x		x	x
OE.User							x			x		x	x
OE.Genuine_Wallet	x			x	x	x	x		x				
OE.Card_Delete			x										

## 6. Security Functional Requirements

### 6.1. SFR supporting definitions

#### 6.1.1. Security Functional Policies (SFP)

Access Control SFPs are given in the table below:

Authentica- tion_SFP	Authentication policy enforcing authentication, re-authentication and authorization rules as defined by OT.User_Auth.  This SFP includes information flows between the Secure Enclave and the biometric sensor (for biometric authentication) and between the TOE and S.iPhone (to enable Optic ID for TOE unlock after the device is turned on or restarted).
Payment_SFP	Security policy enforcing that processing a payment requires the User to confirm the intent to pay and being re-authenticated (passcode, or, if configured, Biometrics) to allow processing of the related data and its exportation.
Card_Perso_SFP	Security policy enforcing that: <ul style="list-style-type: none"><li>• Importing D.Card_Data is only allowed if a passcode is configured</li><li>• Confidential parts of the card data are protected before being sent to the Apple servers</li><li>• Confidential parts of the card data are not imported in Apple Wallet</li></ul>

#### 6.1.2. Subjects and Objects

Objects are the Assets identified in Section 4.1.

Subjects are listed in Sections 4.2 and 4.4

#### 6.1.3. Security Attributes

Security Attribute		
<b>Card Data Confidential parts</b>	Parts of the Card Data that should stay confidential and not been stored in Apple Wallet	<ul style="list-style-type: none"><li>- Secret parts of the card number</li><li>- CVV</li><li>- ...</li></ul>
<b>User Authorization</b>	Part of D.Payment_Data specifying the explicit authorization of the S.User	<ul style="list-style-type: none"><li>- "yes"</li><li>- "no"</li></ul>
<b>Erase Data</b>	Part of D.User_Configuration which, when enabled, erases the data on the device after 10 consecutive attempts to unlock it using the wrong passcode.	<ul style="list-style-type: none"><li>- "enabled"</li><li>- "disabled" (default)</li></ul>
<b>BioAuth Unlock</b>	Part of D.User_Configuration, authorization to use biometric authentication for unlocking a device, "selected" or "not selected" by the User.	<ul style="list-style-type: none"><li>- "selected"</li><li>- "not selected" (default)</li></ul>

Security Attribute		
<b>BioAuth AP</b>	Part of D.User_Configuration, authorization to use biometric authentication for Apple Pay operations, "selected" or "not selected" by the User.	<ul style="list-style-type: none"> <li>- "selected" (default)</li> <li>- "not selected"</li> </ul>
<b>iPhone enable Optic ID</b>	Authorization to use the paired iPhone to enable the use of Optic ID to unlock the TOE after it is turned on or restarted	<ul style="list-style-type: none"> <li>- "enabled"</li> <li>- "disabled" (default)</li> </ul>
<b>Apple OS public key</b>	The public key used to check the authenticity of a new version of D.OS.	<ul style="list-style-type: none"> <li>- Part of installed D.OS</li> </ul>
<b>OS_signature</b>	Part of the OS file that is checked by the TOE before updating D.OS	<ul style="list-style-type: none"> <li>- Part of the update file</li> </ul>
<b>Passcode_off</b>	Part of D.SEP_Configuration, configuration of the OS allowing to use the device without any authentication. When enabled, the TSF should disable biometric authentication and Apple Pay.	<ul style="list-style-type: none"> <li>- "disabled" (default)</li> <li>- "enable"</li> </ul>

#### 6.1.4. Writing conventions for the SFR operations

Iterations are identified by a slash character "/" followed by the name of the iteration.

Assignments and selections are done with *italicized text*.

Refinements are identified with the prefix "Refinement:".

## 6.2. Identification and authentication

### 6.2.1. User authentication

#### FIA\_UID.2 User identification before any action

FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
-------------	--

#### FIA\_UAU.2 User authentication before any action

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
-------------	---

Note: this gives S.User the role of "Authenticated User". According to this requirement, S.User is authenticated by the TSF before performing any of the operations listed in the following requirements.

#### FIA\_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1	The TSF shall provide <i>passcode authentication</i> , <i>biometric authentication (Optic ID)</i> to support user authentication.
-------------	---

FIA_UAU.5.2	<p>The TSF shall authenticate any user's claimed identity according to the:</p> <ul style="list-style-type: none"> <li>• <i>Passcode authentication as default authentication</i></li> <li>• <i>Biometric authentication for:</i> <ul style="list-style-type: none"> <li>- <i>Unlock the device if selected in the "Optic ID &amp; Passcode" configuration setting (BioAuth Unlock = selected)</i></li> <li>- <i>Transaction authorization if selected in the "Optic ID &amp; Passcode" configuration setting (BioAuth AP = selected)</i></li> </ul> </li> <li>• <i>Rules defined in FIA_UAU.6 Re-authenticating and FIA_AFL.1 (Biometric/Erase/Delay) Authentication failure handling.</i></li> </ul>
-------------	--

#### FIA\_AFL.1/Biometric Authentication failure handling

FIA_AFL.1.1 /Biometric	The TSF shall detect when 5 (five) unsuccessful authentication attempts occur related to <i>Biometric validation</i> .
FIA_AFL.1.2 /Biometric	When the defined number of unsuccessful authentication attempts has been met, the TSF shall <i>require Passcode validation, blocking further Biometric validation attempts.</i>

#### FIA\_AFL.1/Erase Authentication failure handling

FIA_AFL.1.1 /Erase	The TSF shall detect when 10 (ten) unsuccessful authentication attempts occur related to <i>passcode validation</i> .
FIA_AFL.1.2 /Erase	When the defined number of unsuccessful authentication attempts has been met, the TSF shall <i>erase data on iPhone if "Erase Data" = enabled.</i>

#### FIA\_AFL.1/Delay Authentication failure handling

FIA_AFL.1.1 /Delay	The TSF shall detect when 3 (three) unsuccessful authentication attempts occur related to <i>passcode validation</i> .
FIA_AFL.1.2 /Delay	When the defined number of unsuccessful authentication attempts has been met, the TSF shall <i>start delaying further passcode validation attempts and require passcode validation.</i>

#### FIA\_UAU.6 Re-authenticating

FIA_UAU.6.1	<p>The TSF shall re-authenticate the user under the conditions <i>that the user requests</i>:</p> <ul style="list-style-type: none"> <li>• <i>OS update (change of D.OS)</i></li> <li>• <i>"Optic ID &amp; Passcode" configuration change (once for all "Optic ID &amp; Passcode" parameters until "Optic ID &amp; Passcode" interface is closed), including "BioAuth Unlock", "BioAuth AP", passcode and Biometric patterns</i></li> <li>• <i>Transaction validation (export of D.Payment_Data), the re-authentication should be done during the 60 seconds after the transaction validation request.</i></li> </ul>
-------------	---

## 6.2.2.Data Authentication

#### FDP\_DAU.1 Basic Data Authentication

FDP_DAU.1.1	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of <i>D.Payment_Data (including S.Merchant and S.User data)</i> .
FDP_DAU.1.2	The TSF shall provide S.SE with the ability to verify evidence of the validity of the indicated information.

### 6.2.3. User attribute definition

#### FIA\_ATD.1 User attribute definition

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: <i>D.User_Passcode, D.User_Bio, D.Card_Data, BioAuth Unlock, BioAuth AP, iPhone enable Optic ID.</i>
<i>Application Note:</i> The update of D.OS shall not modify these user attributes.	

### 6.2.4. Specification of secrets

#### FIA\_SOS.2 TSF Generation of secrets

FIA_SOS.2.1	The TSF shall provide a mechanism to generate secrets that meet <i>FIPS 140-3 validated cryptographic module</i> .
FIA_SOS.2.2	The TSF shall be able to enforce the use of TSF generated secrets for <i>creation of the D.Enable-OpticID_Secret during the Nearby iPhone enables Optic ID Setup</i> .

## 6.3. Access/Flow Control SFRs

### 6.3.1. Authentication\_SFP

#### FDP\_ACC.2/Authentication\_SFP Complete access control

FDP_ACC.2.1/ Authentica- tion_SFP	The TSF shall enforce the <i>Authentication_SFP</i> on:	
	Subjects:	<i>S.User, S.iPhone</i>
	Objects:	<i>the TSF</i>
and all operations among subjects and objects covered by the SFP.		
FDP_ACC.2.2/ Authentica- tion_SFP	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.	

#### FDP\_ACF.1/Authentication\_SFP Security attribute-based access control

FDP_ACF.1.1/ Authentication_SFP	The TSF shall enforce the <i>Authentication_SFP</i> to objects based on the following:	
	Subjects:	<i>S.User, S.iPhone</i>
	Objects:	<i>the TSF</i>
	Security attributes:	<i>"iPhone enable Optic ID"</i>
FDP_ACF.1.2/ Authentication_SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <i>S.User is authenticated according to FIA_UAU.5</i>	
FDP_ACF.1.3/ Authentication_SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: <i>If "iPhone enable Optic ID" is set to "enabled", S.iPhone is running iOS 17.1 or later, S.User has signed into the TOE and S.iPhone using the same Apple Account, and S.iPhone is nearby S.iPhone can enable the use of Optic ID to unlock the TOE when the TOE is turned on or restarted</i>	
FDP_ACF.1.4/ Authentication_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: <i>Optic ID cannot be used for the first unlock immediately after the TOE is turned on or restarted if the conditions referred to in FDP_ACF.1.3/Authentication_SFP are not met</i>	



### FDP\_ITT.1 Basic internal transfer protection

FDP_ITT.1.1	The TSF shall enforce the <i>Authentication_SFP</i> to prevent the <i>modification</i> of user data when it is transmitted between physically-separated parts of the TOE.
-------------	---

Note: This requirement concerns the protection of biometric data sent by the biometric sensor to the Secure Enclave. Protection against modification also includes protection against replay.

## 6.3.2.Payment\_SFP

### FDP\_ETC.2/Transaction Export of user data with security attributes

FDP_ETC.2.1 /Transaction	The TSF shall enforce the <i>Payment_SFP</i> when exporting user data, controlled under the SFP(s), outside of the TOE.
FDP_ETC.2.2 /Transaction	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3 /Transaction	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.
FDP_ETC.2.4 /Transaction	The TSF shall enforce the following rules when user data is exported from the TOE: <ul style="list-style-type: none"> <li>- <i>exported Payment_SFP details (the card to be used from Apple Wallet, the amount and the payee in the case of e-commerce payments) are those displayed to S.User during re-authentication request (FIA_UAU.6 Re-authenticating)</i></li> <li>- <i>D.Payment_Data includes a unique identifier (An Apple Pay server nonce)</i></li> </ul>

### FDP\_ACC.2/Payment\_SFP Complete access control

FDP_ACC.2.1/ Payment_SFP	The TSF shall enforce the <i>Payment_SFP</i> on: <table border="1"> <tr> <td>Subjects:</td><td><i>S.User</i></td></tr> <tr> <td>Objects:</td><td><i>D.Payment_Data (including S.User and S.Merchant Data)</i></td></tr> </table> and all operations among subjects and objects covered by the SFP.	Subjects:	<i>S.User</i>	Objects:	<i>D.Payment_Data (including S.User and S.Merchant Data)</i>
Subjects:	<i>S.User</i>				
Objects:	<i>D.Payment_Data (including S.User and S.Merchant Data)</i>				
FDP_ACC.2.2/ Payment_SFP	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.				

Note: the only possible operation on D.Payment\_Data is to export it as a transaction order to the Secure Element.

### FDP\_ACF.1/Payment\_SFP Security attribute based access control

FDP_ACF.1.1/ Payment_SFP	The TSF shall enforce the <i>Payment_SFP</i> to objects based on the following: <table border="1"> <tr> <td>Subjects:</td><td><i>S.User</i></td></tr> <tr> <td>Objects:</td><td><i>D.Payment_Data (including S.User and S.Merchant Data), the Secure Element (through a trusted channel)</i></td></tr> <tr> <td>Security attributes:</td><td><i>"User Authorization", "BioAuth AP", "Passcode_off"</i></td></tr> </table>	Subjects:	<i>S.User</i>	Objects:	<i>D.Payment_Data (including S.User and S.Merchant Data), the Secure Element (through a trusted channel)</i>	Security attributes:	<i>"User Authorization", "BioAuth AP", "Passcode_off"</i>
Subjects:	<i>S.User</i>						
Objects:	<i>D.Payment_Data (including S.User and S.Merchant Data), the Secure Element (through a trusted channel)</i>						
Security attributes:	<i>"User Authorization", "BioAuth AP", "Passcode_off"</i>						
FDP_ACF.1.2/ Payment_SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: <ul style="list-style-type: none"> <li>- <i>Export of D.Payment_Data with "User Authorization" set to "yes" to the Secure Element is allowed if:</i> <ul style="list-style-type: none"> <li>- <i>S.User shows their intent to pay (double clicking the top button)</i></li> <li>- <i>S.User had been successfully re-authenticated for transaction validation (FIA_UAU.6).</i></li> </ul> </li> </ul>						
FDP_ACF.1.3/ Payment_SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: <i>none</i> .						
FDP_ACF.1.4/ Payment_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: <i>"Passcode_off" is "enabled"</i> .						



### 6.3.3.Card\_Perso\_SFP

#### FDP\_ACC.2/Card\_Perso\_SFP Complete access control

FDP_ACC.2.1 /Card_Perso_SF P	The TSF shall enforce the <i>Card_Perso_SFP</i> on	
	Subjects:	<i>S.User, S.Apple_Servers</i>
	Objects:	<i>D.Card_Data</i>
	and all operations among subjects and objects covered by the SFP.	
FDP_ACC.2.2 /Card_Perso_SF P	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.	

#### FDP\_ACF.1/Card\_Perso\_SFP Security attribute-based access control

FDP_ACF.1.1 /Card_Perso_SFP	The TSF shall enforce the <i>Card_Perso_SFP</i> to objects based on the following:	
	Subjects:	<i>S.User, S.Apple_Servers</i>
	Objects:	<i>D.Card_Data</i>
	Security attributes:	<i>Passcode_off</i>
FDP_ACF.1.2 /Card_Perso_SFP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: - <i>S.User is connected to its iCloud account, and is authenticated on the TOE.</i>	
FDP_ACF.1.3 /Card_Perso_SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: <i>none</i> .	
FDP_ACF.1.4 /Card_Perso_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: <i>"Passcode_off" is enabled.</i>	

#### FDP\_ETC.2/Card\_Perso\_SFP Export of user data with security attributes

FDP_ETC.2.1 /Card_Perso_SFP	The TSF shall enforce the <i>Card_Perso_SFP</i> when exporting user data, controlled under the SFP(s), outside of the TOE.	
FDP_ETC.2.2 /Card_Perso_SFP	The TSF shall export the user data with the user data's associated security attributes.	
FDP_ETC.2.3 /Card_Perso_SFP	The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.	
FDP_ETC.2.4 /Card_Perso_SFP	The TSF shall enforce the following rules when user data is exported from the TOE: - <i>D.Card_Data is encrypted before being exported to S.Apple_Servers</i> - <i>"Card Data Confidential parts" are not kept on the TOE after being exported.</i>	

#### FPT\_ITC.1 Inter-TSF confidentiality during transmission

FPT_ITC.1.1	The TSF shall protect all TSF data transmitted from the TSF to another trusted IT product from unauthorised disclosure during transmission.
-------------	---

#### FDP\_ITC.1 Import of user data without security attributes

FDP_ITC.1.1	The TSF shall enforce the <i>Card_Perso_SFP</i> when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: <i>None</i> .

Note: security attributes of the Card Data are "Card Data Confidential parts" in section 6.1.3. These requirements specify that the confidential part of the cards data is used for card enrollment (FDP\_ETC.2/Card\_Perso\_SFP) but are not stored on the TOE.

## 6.4. Secure Enclave/Secure Element Trusted Channel

#### FTP\_ITC.1/SE Inter-TSF trusted channel

FTP_ITC.1.1/SE	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SE	The TSF shall permit <i>the TSF</i> to initiate communication via the trusted channel.
FTP_ITC.1.3/SE	The TSF shall initiate communication via the trusted channel for <i>Payment initiation and transmission of D.Payment_Data</i> .

#### FDP\_UCT.1/SE Basic data exchange confidentiality

FDP_UCT.1.1/SE	The TSF shall enforce the <i>Payment_SFP</i> , to <i>transmit</i> user data in a manner protected from unauthorised disclosure.
----------------	---

#### FDP\_UIT.1/SE Data exchange integrity

FDP_UIT.1.1/SE	The TSF shall enforce the <i>Payment_SFP</i> , to <i>transmit and receive</i> user data in a manner protected from <i>modification, insertion and replay</i> errors.
FDP_UIT.1.2/SE	The TSF shall be able to determine on receipt of user data, whether <i>modification, insertion or replay</i> has occurred.

#### FPT\_RPL.1/SE Replay detection

FPT_RPL.1.1/SE	The TSF shall detect replay for the following entities: <i>S.SE</i> .
FPT_RPL.1.2/SE	The TSF shall perform <i>reject data</i> when replay is detected.

## 6.5. Secure Enclave/iPhone Trusted Channel

#### FTP\_ITC.1/iPhone Inter-TSF trusted channel

FTP_ITC.1.1/iPhone	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/iPhone	The TSF shall permit <i>the TSF</i> to initiate communication via the trusted channel.
FTP_ITC.1.3/iPhone	The TSF shall initiate communication via the trusted channel for: <i>enable Optic ID to unlock the TOE after the TOE is turned on or restarted</i> .

#### FDP\_UCT.1/iPhone Basic data exchange confidentiality

FDP_UCT.1.1/iPhone	The TSF shall enforce the <i>Authentication_SFP</i> , to <i>transmit and receive</i> user data in a manner protected from unauthorised disclosure.
--------------------	--

#### FDP\_UIT.1/iPhone Data exchange integrity

FDP_UIT.1.1/iPhone	The TSF shall enforce the <i>Authentication_SFP</i> to <i>transmit and receive</i> user data in a manner protected from <i>modification, insertion and replay</i> errors.
FDP_UIT.1.2/iPhone	The TSF shall be able to determine on receipt of user data, whether <i>modification, insertion or replay</i> has occurred.

#### FPT\_RPL.1/iPhone Replay detection

FPT_RPL.1.1/iPhone	The TSF shall detect replay for the following entities: <i>S.iPhone</i> .
FPT_RPL.1.2/iPhone	The TSF shall perform <i>reject data</i> when replay is detected.

## 6.6. Local data protection

#### FPR\_UNO.1 Unobservability

FPR_UNO.1.1	The TSF shall ensure that <i>S.Attacker</i> are unable to observe the operation <i>Passcode set, Passcode check, Passcode Update, Passcode removal, Biometrics set, Biometrics check, Biometrics update, Biometrics delete, Apple Pay/Cash Card provisioning, Nearby iPhone enables Optic ID activation</i> , on <i>D.User_Bio, D.User_Passcode, D.Card_Data, D.SEP_iPhone, D.Enable-OpticID_Secret</i> by <i>S.User</i> .
-------------	--

#### FDP\_RIP.1 Subset residual information protection

FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the <i>deallocation of the resource</i> from the following objects: <i>D.User_Bio, D.User_Passcode, "Card Data Confidential parts" and iCloud Account (in D.User_Configuration)</i> .
<i>Application Note:</i> <ul style="list-style-type: none"><li>• The removal of the iCloud Account by <i>S.User</i> triggers the deallocation of all the Apple Pay data/configuration</li><li>• The revocation of an individual card by the card issuer triggers the deallocation of the related card data</li><li>• The procedure of Reset on the device triggers the deallocation of all security attributes except the D.OS</li><li>• The removal of "Card Data Confidential parts" is done by instructing the Secure Element to mark the card as terminated</li><li>• The removal of the passcode by <i>S.User</i> disables the actual passcode; and triggers the deallocation of the iCloud Account information and all the Apple Pay data</li></ul>	

#### FDP\_SDI.1 Stored data integrity monitoring

FDP_SDI.1.1	The TSF shall monitor user data stored in containers controlled by the TSF for <i>integrity errors</i> on all objects, based on the following attributes: <i>D.User_Bio, D.Card_Data, D.OS</i> .
-------------	--

## 6.7. TSF management

### 6.7.1.Roles and Management Functions

#### FMT\_SMR.1 Security roles

FMT_SMR.1.1	The TSF shall maintain the roles <i>Authenticated User</i> .
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

#### FMT\_SMF.1 Specification of Management Functions

FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: <i>management of security attributes</i> (see FMT_MSA.1).
-------------	--

### 6.7.2.Management of security attributes

#### FMT\_MSA.3 Static attribute initialization

FMT_MSA.3.1	The TSF shall enforce the <i>Payment_SFP</i> , <i>Card_Perso_SFP</i> to provide	
	<b>"BioAuth Unlock"</b>	restrictive (disabled)
	<b>"BioAuth AP"</b>	permissive (selected)
	<b>"Passcode_off"</b>	restrictive (disabled)
	<b>"iPhone enable Optic ID"</b>	restrictive (disabled)
	<b>"Erase Data"</b>	permissive (disabled)
default values for security attributes that are used to enforce the SFP.		
FMT_MSA.3.2	The TSF shall allow <i>nobody</i> to specify alternative initial values to override the default values when an object or information is created.	

#### FMT\_MSA.1 Management of security attributes

FMT_MSA.1.1	The TSF shall enforce the <i>Authentication_SFP</i> , <i>Card_Perso_SFP</i> to restrict the ability to <i>modify</i> the security attributes " <i>"BioAuth Unlock"</i> , " <i>BioAuth AP"</i> , " <i>Passcode_off"</i> , " <i>Erase Data"</i> , " <i>iPhone enable Optic ID"</i> , to " <i>Authenticated User"</i>
<i>Application Note:</i>	
<ul style="list-style-type: none"><li>When "<i>Passcode_off"</i> is enabled, the TSF removes the D.Card_Data according to FDP_RIP.1.</li></ul>	

### 6.7.3.Management of TSF Data

#### FMT\_MTD.1 Management of TSF data

FMT_MTD.1.1	The TSF shall restrict the ability to <i>update</i> the <i>D.OS</i> to <i>"Authenticated user"</i> .
-------------	--

#### FMT\_MTD.3 Secure TSF data

FMT_MTD.3.1	The TSF shall ensure that only secure values are accepted for <i>D.OS</i> .
<i>Application Note:</i> secure value is defined by <i>"OS_signature"</i> is valid and signed by <i>"Apple OS public key"</i> .	

## 6.8. Security Requirements Rationale

### 6.8.1. Security Functional Requirements (SFR) Dependencies

TOE SFR	Required dependencies	Covered by
<b>FIA_UAU.2</b>	FIA_UID.1	FIA_UID.2
<b>FIA_AFL.1 (Bio-metric/Erase/Delay)</b>	FIA_UAU.1	FIA_UAU.2
<b>FDP_ACC.2/Authentication_SFP</b>	FDP_ACF.1	FDP_ACF.1/Authentication_SFP
<b>FDP_ACF.1/Authentication_SFP</b>	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2/Authentication_SFP FMT_MSA.3
<b>FDP_ACC.2/Payment_SFP</b>	FDP_ACF.1	FDP_ACF.1/Payment_SFP
<b>FDP_ACF.1/Payment_SFP</b>	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2/Payment_SFP FMT_MSA.3
<b>FDP_ITT.1</b>	FDP_ACC.1, or FDP_IFC.1	FDP_ACC.2/Authentication_SFP
<b>FDP_ETC.2/Transaction</b>	FDP_ACC.1, or FDP_IFC.1	FDP_ACC.2/Payment_SFP
<b>FDP_ACC.2/Card_Perso_SFP</b>	FDP_ACF.1	FDP_ACF.1/Card_Perso_SFP
<b>FDP_ACF.1/Card_Perso_SFP</b>	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2/Card_Perso_SFP FMT_MSA.3
<b>FDP_ITC.1</b>	FDP_ACC.1, or FDP_IFC.1 FMT_MSA.3	FDP_ACC.2/Card_Perso_SFP FMT_MSA.3
<b>FDP_ETC.2/Card_Perso_SFP</b>	FDP_ACC.1, or FDP_IFC.1	FDP_ACC.2/Card_Perso_SFP
<b>FDP_UCT.1/SE</b>	FDP_ACC.1, or FDP_IFC.1  FTP_ITC.1, or FTP_TRP.1	FDP_ACF.1/Payment_SFP, and FDP_ACF.1/Card_Perso_SFP FTP_ITC.1/SE
<b>FDP_UIT.1/SE</b>	FDP_ACC.1, or FDP_IFC.1  FTP_ITC.1, or FTP_TRP.1	FDP_ACF.1/Payment_SFP, and FDP_ACF.1/Card_Perso_SFP FTP_ITC.1/SE
<b>FDP_UCT.1/iPhone</b>	FDP_ACC.1, or FDP_IFC.1 FTP_ITC.1, or FTP_TRP.1	FDP_ACF.1/Authentication_SFP FTP_ITC.1/iPhone
<b>FDP_UIT.1/iPhone</b>	FDP_ACC.1, or FDP_IFC.1 FTP_ITC.1, or FTP_TRP.1	FDP_ACF.1/Authentication_SFP FTP_ITC.1/iPhone
<b>FMT_SMR.1</b>	FIA_UID.1	FIA_UID.2
<b>FMT_MSA.3</b>	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
<b>FMT_MSA.1</b>	FDP_ACC.1, or FDP_IFC.1  FMT_SMR.1, SMT_SMF.1	FDP_ACC.2/Authentication_SFP, FDP_ACC.2/Authentication_SFP, and FDP_ACC.2/Card_Perso_SFP FMT_SMR.1, FMT_SMF.1
<b>FMT_MTD.1</b>	FMT_SMR.1, SMT_SMF.1	FMT_SMR.1, SMT_SMF.1
<b>FMT_MTD.3</b>	FMT_MTD.1	FMT_MTD.1

Requirements without dependency: FIA\_UID.2, FIA\_SOS.2, FIA\_UAU.6, FIA\_UAU.5, FDP\_DAU.1, FIA\_ATD.1, FPT\_ITC.1, FTP\_ITC.1/SE, FPT\_RPL.1/SE, FTP\_ITC.1/iPhone, FPT\_RPL.1/iPhone, FPR\_UNO.1, FDP\_RIP.1, FMT\_SMF.1 and FDP\_SDI.1

## 6.8.2.Rationale SFR/Security Objectives for the TOE

Objective reference	Rationale
<b>OT.User_Auth</b>	<p>FIA_UID.2 and FIA_UAU.2 enforce each User of the device is authenticated before being able to do any action in the user interface.</p> <p>FIA_UAU.5 specifies different authentication methods.</p> <p>FIA_UAU.6 enforces a re-authentication for the OS update, for changing the authentication configuration, including biometric data management and biometric authentication policy or for a transaction validation.</p> <p>FMT_SMR.1 and FMT_SMF.1 SF ensure that the TSF shall maintain the roles Authenticated User and be capable of performing the management functions.</p> <p>FIA_ATD.1, FMT_MSA.3, FMT_MSA.1 and FMT_MTD.1 specify the management of related information.</p> <p>FMT_MTD.3 specifies the signature verification on the OS update.</p> <p>FIA_AFL.1/Biometric, FIA_AFL.1/Erase, and FIA_AFL.1/Delay specify the failure handling in case of wrong biometric or passcode authentication.</p> <p>FPR_UNO.1 ensures the non-observability of the passcode.</p> <p>FDP_ITT.1 also support this objective ensuring the biometric data is not modified during internal transfer.</p>
<b>OT.Card_Data</b>	<p>The SFP Card_Perso_SFP and the associated SFRs (FDP_ACC.2/Card_Perso_SFP, FDP_ACF.1/Card_Perso_SFP, FDP_ITC.1 and FDP_ETC.2/Card_Perso_SFP, FPT_ITC.1) enforce card data stored in Apple Wallet does not include sensitive card data, which is only sent to the Secure Element.</p> <p>FPT_ITC.1/SE, FDP_UCT.1/SE and FDP_UIT.1/SE enforce that all the data exchanged between the TSF and S.SE is protected (with their corresponding security property) by a trusted channel.</p> <p>FPR_UNO.1 ensures the non-observability of secret card data.</p> <p>FDP_SDI.1 ensures card data stored in containers controlled by the TSF are monitored for integrity errors.</p>
<b>OT.Passcode_Delete</b>	<p>FDP_ACC.2/Card_Perso_SFP and FDP_ACF.1.4/Card_Perso_SFP enforce the card enrollment is not possible if Passcode_off is enabled.</p> <p>FIA_UAU.6 enforces a re-authentication for changing the Passcode_off configuration.</p> <p>FPR_UNO.1 ensures the non-observability of the passcode.</p>
<b>OT.Card_Delete</b>	<p>FDP_RIP.1 ensures the confidential parts of the card data are securely removed by the Secure Element.</p> <p>Refinement of FMT_MSA.1.1 ensures the secure delete in case of passcode turning off.</p> <p>FPR_UNO.1 ensures the non-observability of sensitive card data.</p>
<b>OT.Auth_SE</b>	<p>FIA_UID.2, FIA_UAU.2, FIA_UAU.5 specify the base of the authentication feature.</p> <p>FIA_AFL.1/Biometric enhance the biometric security limiting the authentication attempts before requiring passcode authentication.</p> <p>FIA_AFL.1/Erase and FIA_AFL.1/Delay protect the TSF and the user data against brute force attacks.</p> <p>FIA_UAU.6 specifies the re-authentication for some functions of the TOE.</p>

Objective reference	Rationale
<b>OT.Payment</b>	FDP_ETC.2.4/Transaction ensures the transaction details are displayed before a transaction is validated by the User. FIA_UAU.6 ensures each transaction is validated by a re-authentication. FDP_DAU.1 provides evidence of the validity of Apple Pay Transaction Data, verifiable by the card issuer. FDP_ACC.2/Payment_SFP and FDP_ACF.1/Payment_SFP ensure user authorization is done before each transaction. FPT_RPL.1/SE ensures transaction replay detection.
<b>OT.Bio_Delete</b>	FDP_RIP.1 ensures biometric data delete is erased securely.
<b>OT.Device_Reset</b>	FDP_RIP.1 ensures all sensitive data is securely removed during a device reset.
<b>OT.Anti_Replay</b>	FDP_ETC.2.4/Transaction ensures a unique identifier provided by the Apple server is included in the transaction data, avoiding any replay attack.
<b>OT.OS_Update</b>	FIA_UAU.6.1 ensures S.User is re-authenticated before the OS update proceeds. FIA_ATD.1.1 ensures that all the user data with impact on the TSF behavior are not modified during the OS update process. FDP_SDI.1 ensures D.OS stored in containers controlled by the TSF is monitored for integrity errors.
<b>OT.iPhone</b>	FPT_ITC.1/iPhone, FDP_UCT.1/iPhone, FDP_UIT.1/iPhone, FIA_SOS.2, FPR_UNO.1 and FPT_RPL.1/iPhone enforce that the confidentiality and integrity of all the data exchanged between the TSF and S.iPhone is protected using a trusted channel. The protected operations are specified by FDP_ACC.2/Authentication_SFP and FDP_ACF.1/Authentication_SFP.

### 6.8.3.SAR Dependencies

TOE SAR	Dependencies
<b>ADV_ARC.1</b>	ADV_FSP.1, ADV_TDS.1
<b>ADV_FSP.3</b>	ADV_TDS.1
<b>ADV_TDS.1</b>	ADV_FSP.2
<b>AGD_OPE.1</b>	ADV_FSP.1
<b>AGD_PRE.1</b>	No dependencies
<b>ALC_CMC.2</b>	ALC_CMS.1
<b>ALC_CMS.2</b>	No dependencies
<b>ALC_DEL.1</b>	No dependencies
<b>ALC_FLR.3</b>	No dependencies
<b>ASE_CCL.1</b>	ASE_INT.1, ASE_ECD.1, ASE_REQ.1
<b>ASE_ECD.1</b>	No dependencies
<b>ASE_INT.1</b>	No dependencies
<b>ASE_OBJ.2</b>	ASE_SPD.1
<b>ASE_REQ.2</b>	ASE_OBJ.2, ASE_ECD.1
<b>ASE_SPD.1</b>	No dependencies

TOE SAR	Dependencies
<b>ASE_TSS.1</b>	ASE_INT.1, ASE_REQ.1, ADV_FSP.1
<b>ATE_COV.1</b>	ADV_FSP.2, ATE_FUN.1
<b>ATE_FUN.1</b>	ATE_COV.1
<b>ATE_IND.2</b>	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1
<b>AVA_VAN.2</b>	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

All the dependencies are covered.

#### 6.8.4. SAR Rationale

For this evaluation, the SARs of EAL2 have been chosen as they provide assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behavior. It was established that this level is appropriate for the model of attack of Apple Pay.

ADV\_FSP.3 augmentation has been chosen to enhance the level of information provided related to SFR-enforcing TSFIs and provide a complete summary of the TOE.

ALC\_FLR.3 augmentation has been chosen to guarantee the security of the security functions in the scope of this security target during the maintenance of the TOE.



# 7. TOE Summary Specification

This section describes the security functions of the TOE covering the SFR of the previous chapter.

## 7.1. SF User authentication and management

When using the TOE, before being able to use Optic ID as a Biometric authentication method, the device must be set up so that a passcode is required to unlock it.

Optic ID is Apple’s authentication system that enables secure access to a Vision Pro device equipped with the eye-tracking system of LEDs and infrared cameras. This technology is based on the Optic ID sensor and the Secure Enclave.

When the Secure Enclave detects a successful match against the stored mathematical representation, the device unlocks without asking for the device passcode. Optic ID does not replace the passcode but provides easy access to the device within defined boundaries and time constraints. To use Optic ID, the device must be set up so that a passcode is required to unlock it.

The passcode can always be used instead of Biometrics and the passcode is required under the following circumstances:

- The device has just been turned on or restarted (does not apply if the feature “Nearby iPhone enables Optic ID” is used)
- The User has not unlocked their device for more than 48 hours
- The User has not used their passcode to unlock their device for 156 hours (six and a half days) and the User has not used a biometric to unlock their device in 4 hours
- There were five unsuccessful biometric match attempts (though for usability, the device might offer entering a passcode instead of using biometrics after a smaller number of failures)

If the User is signed in to their iPhone with iOS 17.1 or later and the TOE with the same Apple Account, having their iPhone nearby can enable Optic ID when they turn on or restart their TOE device. To enable this feature, the User shall:

1. Navigate to Settings > Optic ID & Passcode.
2. Tap their iPhone below “Nearby iPhone Enables Optic ID”.

The feature can be used if the User’s iPhone is nearby, and the iPhone was last unlocked in the past hour.

These features implement the requirements listed in §6.2 and in §6.3.1 for the authentication, in §6.6 for local data protection and in FMT\_SMF.1, FMT\_MSA.1, and FMT\_MSA.3 for management.

The following table summarizes the functions supporting User authentication.

Function	Description
Passcode authentication	Passcode_Setup: Setup of the device’s passcode.
	Passcode_Update: Update of the device’s passcode.
	Passcode_Verify: Authentication of the User using their passcode.
	Passcode_Delete: Removal of the passcode
Biometric authentication	Bio_Enroll: Enrollment of biometrics credential (first, or additional).
	Bio_Update: Update of Biometrics.
	Bio_Verify: Authentication of the User using Biometrics.
	Bio_Delete: Delete an enrolled Biometrics credential (one, or all).

Function	Description
Nearby iPhone enables Optic ID	iPhone_Enables_Optic_ID_Setup: Enable the feature "Nearby iPhone enables Optic ID".
	iPhone_Enables_Optic_ID_Check: Secure process to import the Secret to the TOE's Secure Enclave for enabling Optic ID the device.

### 7.1.1.Passcode\_Setup

The TOE offers a configuration setting where the User can set up a passcode that will be used to perform authentication in order to access restricted services on the device: device unlock, Apple Pay transactions, Apple Pay Transfers, and more. The TOE enforces strong access control in order to prevent access to these restricted services without authentication (FIA\_UID.2).

*Note: The User has the possibility to use the passcode or any other activated (with enrolled templates) authentication method to perform unlock<sup>4</sup>, Apple Pay transactions and Apple Cash transfers.*

The TOE ensures the non-observability of the passcode during the setting process within the Secure Enclave (FPR\_UNO.1).

### 7.1.2.Passcode\_Verify

The TOE offers passcode entry to the User as part of the device unlock procedure, or during the User authorization step of an Apple Pay transaction or Apple Cash transfer. The User might have selected the default method as being Biometrics, but passcode verification is always possible (as a fallback or by User choice). The TSFs ensure that passcode verification preserves the secrecy of the passcode value set by the User, which is expected in order to prevent an attacker from guessing the code by observing the verification process (FPR\_UNO.1). The TOE ensures that the verification process would not validate a code that does not match the passcode set by the User and detect alterations to the configured value (FDP\_SDI.1), preventing use of the User account (and related data) and forcing a device panic. To discourage brute-force passcode attacks, the TOE authentication failure policy is escalating time delays after the entry of an invalid passcode (FIA\_AFL.1/Delay) or to erase data after 10 attempts if the feature "Erase data" is enabled (FIA\_AFL.1/Erase).

### 7.1.3.Passcode\_Update

The User can update the passcode value through the device's settings menu. This functions as a verify operation, as knowledge of the previous passcode value is required to proceed to the setup step where the User types a new value and effectively updates the value in the Secure Enclave (FIA\_UAU.2, FDP\_ACC.2/Authentication\_SFP and FDP\_ACF.1/Authentication\_SFP). The TOE ensures the non-observability of the old passcode during the verification as well as of the new passcode during the setting process (FPR\_UNO.1). The TOE also enforces passcode alteration detection, preventing a corrupted passcode from being used to reset the authentication function (FDP\_SDI.1).

### 7.1.4.Passcode\_Delete

If the User wants to fully remove the use of the passcode on the device, because this would not allow an adequate security level for the processing of the TSF, the actual passcode is disabled; and the iCloud

---

<sup>4</sup> The passcode is required to be used for the first unlock after the device is turned on or restarted, unless the feature "Nearby iPhone enables Optic ID" is used

Account information and all the Apple Pay data is deallocated. (FDP\_RIP.1). To prevent misuse of the passcode deletion function, the User is required to first verify the current passcode before proceeding (FIA\_UAU.2, FDP\_ACC.2/Authentication\_SFP and FDP\_ACF.1/Authentication\_SFP), and the TOE protects the passcode secrecy during the verification process in case an attacker was to use this path for attempting an observation-based attack (FPR\_UNO.1).

The Secure Element, in the TOE Environment, is responsible for securely deleting the Apple Pay card data and Apple Cash card data during this process.

### 7.1.5.Bio\_Enroll

The TOE offers Biometric authentication through the Optic ID service. To use Optic ID, the User must set up the device so that a passcode is required to unlock it, and passcode verification is required to be able to perform any modifications to the Biometrics setting. Access to the iris enrollment and the setting for enabling Biometrics for Apple Pay (and Apple Cash), is gated by this passcode verification (FIA\_UAU.2, FDP\_ACC.2/Authentication\_SFP and FDP\_ACF.1/Authentication\_SFP).

### 7.1.6.Bio\_Update

Once iris image data is enrolled on a device, the User can update it within the settings of the Optic ID feature, for which access is gated by the passcode (FIA\_UAU.2, FDP\_ACC.2/Authentication\_SFP and FDP\_ACF.1/Authentication\_SFP). After a successful passcode verification, the User can reset Optic ID, deleting the associated templates, and re-enroll their iris later. This procedure is effectively enforcing the same security principles as a deletion (Bio\_Delete), and an enrollment (Bio\_Enroll): the Secure Enclave ensures that biometric data integrity is preserved, and the deallocation prevents attackers from finding any residual information (FPR\_UNO.1, FDP\_SDI.1, and FDP\_RIP.1).

### 7.1.7.Bio\_Verify

After the device is reset and passcode is entered to allow the device's normal mode of operation, the Biometric authentication function is offered to the User as the default means for authentication, if it is enabled, for device unlock, Apple Pay transactions, and Apple Cash transfers. The User will present their biometric features to the device's biometric sensor, and the Secure Enclave will securely perform the verification of the submitted template to the enrolled biometric template(s). The Secure Enclave ensures the integrity monitoring of the biometric templates during the verification process (FDP\_SDI.1). In case of verification failure, which means the TOE was not able to find a successful match, an authentication failure policy is enforced, and passcode verification is required before the Biometric authentication function is enabled again (FIA\_AFL.1/Biometric).

### 7.1.8.Bio\_Delete

The User has the capability to delete all enrolled Biometrics from the Optic ID settings on the device using the Reset Optic ID option. This function deletes the enrolled template and is gated by the passcode (FIA\_UAU.2, FDP\_ACC.2/Authentication\_SFP and FDP\_ACF.1/Authentication\_SFP). The deletion process ensures that no residual information of the deallocated data is left behind or leaked to a potential observer (FDP\_RIP.1, and FPR\_UNO.1).

### 7.1.9.iPhone\_Enables\_Optic\_ID\_Setup

Optionally, the User can choose to enable the “Nearby iPhone enables Optic ID” feature, provided that their iPhone is running iOS 17.1 or later, and the User is signed in to their iPhone and the TOE device with the same Apple Account. Enabling the feature via the Settings of the TOE device requires the User to enter their passcode (FDP\_ACC.2/Authentication\_SFP, FDP\_ACF.1/Authentication\_SFP, FMT\_MSA.1, and FMT\_MSA.3).

During the feature setup process, the TOE’s Secure Enclave creates a non-predictable Optic ID Enablement Secret, D.EnableOpticID\_Secret (FIA\_SOS.2 and FPR\_UNO.1).

The TOE’s Secure Enclave securely exports D.EnableOpticID\_Secret to the iPhone’s Secure Enclave, using a secure channel to protect the sensitive asset that is established using the Secure Enclave iPhone pairing secret, D.SEP\_iPhone (FPT\_ITC.1/iPhone, FDP\_UCT.1/iPhone, FDP\_UIT.1/iPhone, FPT\_RPL.1/iPhone).

While the feature is enabled, the TOE maintains the security attributes and assets of the “Nearby iPhone enables Optic ID” process, including the asset D.EnableOpticID\_Secret (FIA\_ATD.1).

### 7.1.10.iPhone\_Enables\_Optic\_ID\_Check

Optionally, if the User enables the “Nearby iPhone enables Optic ID” feature, Optic ID can be used for the first TOE unlock after it is turned on or restarted when the User’s iPhone is nearby.

During this process, the iPhone transmits the Optic ID Enablement Secret, D.EnableOpticID\_Secret, which the TOE receives and imports into its Secure Enclave for verification. During transmission of D.EnableOpticID\_Secret, the TOE applies security measures to protect the sensitive asset via a secure channel established using the Secure Enclave iPhone pairing secret, D.SEP\_iPhone (FPT\_ITC.1/iPhone, FDP\_UCT.1/iPhone, FDP\_UIT.1/iPhone, FPT\_RPL.1/iPhone).

## 7.2. SF Biometric/Secure Enclave secure channel

The TSF protects the data exchanged between the biometric sensor and the Secure Enclave against modification (FDP\_ITT.1). The biometric sensor and the Secure Enclave are paired during manufacturing to enable this secure communication.

## 7.3. SF Secure Enclave/Secure Element secure channel

The TSF is able to initialize a secure channel with the Secure Element (FPT\_ITC.1/SE). This secure channel protects the exchanged data with its corresponding security properties: against disclosure (FDP\_UCT.1/SE), modification (FDP\_UIT.1/SE) and replay (FPT\_RPL.1/SE).

## 7.4. SF Secure Enclave/iPhone secure channel

The TSF is able to initialize a secure channel to S.iPhone (FPT\_ITC.1/iPhone). This secure channel protects the exchanged data against disclosure (FDP\_UCT.1/iPhone), modification (FDP\_UIT.1/iPhone) and replay (FPT\_RPL.1/iPhone).

## 7.5. SF Card Data management

The following table summarizes the functions supporting Card Data management.

Function	Description
Apple Pay card data management	AP_Card_Provisioning: Provisioning of a new card for Apple Pay.
	AP_Cancellation: User removes a card from Apple Wallet.
	AP_Revocation: card issuer initiated suspend/unlink of a payment card in Apple Wallet.
Apple Cash card data management	APC_Enroll: Enroll in Apple Cash services.
	APC_Disenroll: User cancels their enrollment in Apple Cash services.
	APC_Revocation: card issuer initiated suspend/unlink of user's Apple Cash services.

### 7.5.1.AP\_Card\_Provisioning

On the TOE, there are different ways to add a card into Apple Wallet:

- Adding a card manually
- Adding cards on file from an iTunes Store account to Apple Pay
- Adding cards from a card issuer's app
- Adding cards from a card issuer's website (only for Apple Pay, not available for Apple Cash)
- Adding cards that were provisioned on a different device (multi-device provisioning)

The first three modes are only available to an authenticated User on the device, with the passcode enabled (FIA\_UAU.2, FDP\_ACC.2/Card\_Perso\_SFP, and FDP\_ACF.1/Card\_Perso\_SFP).

With the Multi-device provisioning feature, when a user provisions an eligible payment card, they will also be able to push provision the card to other Apple Pay-capable devices on the same iCloud account. Nothing is copied from the original device; the other devices provision using the same flow they would use during device setup. The TOE can initiate push provisioning of cards to other devices and can also receive cards that were initiated by provisioning on one of the User's other devices.

When a User adds a card to Apple Wallet, the TSF encrypts card data (FPT\_ITC.1) and sends it to Apple servers (FDP\_ETC.2/Card\_Perso\_SFP). Full card numbers are not stored on the device (FDP\_ITC.1) or on Apple servers.

Integrity protections are in place to prevent alteration of the enrolled Apple Pay card data (FDP\_SDI.1).

### 7.5.2.AP\_Cancellation

When the User decides to remove an Apple Pay card from Apple Wallet, the TSF orders the Secure Element to securely invalidate and remove the Device Account Number (FDP\_RIP.1).

### 7.5.3.AP\_Revocation

When the card issuer decides to suspend or unlink an Apple Pay card from Apple Wallet of a TOE User, the TSF order the Secure Element to securely invalidate and remove the Device Account Number (FDP\_RIP.1).

### 7.5.4.APC\_Enroll

To use person-to-person payments and Apple Cash, a User must be signed into their iCloud account on an Apple Cash compatible device.

The User can add the Apple Cash card from Wallet or Settings. This capability is only available to an authenticated User on a device with passcode enabled. Full card numbers are not stored on the device (FDP\_ITC.1) or on Apple servers. Integrity protections are in place in the TOE to prevent alteration of the enrolled Apple Cash card data (FDP\_SDI.1)

### 7.5.5.APC\_Disenroll

When the User decides to remove an Apple Cash card from Apple Wallet, the TSF order the Secure Element to securely invalidate and remove the Device Account Number (FDP\_RIP.1).

### 7.5.6.APC\_Revocation

When the card issuer decides to suspend or unlink an Apple Cash card from Apple Wallet of a TOE User, the TSF order the Secure Element to securely invalidate and remove the Device Account Number (FDP\_RIP.1).

## 7.6. SF Payment management

When a device initiates an Apple Pay transaction, the Secure Element, in the TOE Environment, only allows a payment to be made after it receives authorization from the Secure Enclave. This involves confirming the User has provided intent and has authenticated with Biometric authentication or using the device passcode (FDP\_ACC.2/Payment\_SFP, FDP\_ACF.1/Payment\_SFP, and FMT\_SMR.1). Biometric authentication is the default method if available, but the passcode can be used at any time. A passcode is automatically offered after three unsuccessful attempts to match biometrics; after five unsuccessful attempts, the passcode is required. A passcode is also required when biometric authentication is not configured or not enabled for Apple Pay (FMT\_SMF.1, FMT\_MSA.1, and FMT\_MSA.3).

Apple Pay includes an anti-replay mechanism that prevents transactions to be repeated by including an Apple Pay server nonce (also known as a Transaction Token) in D.Payment\_Data.

The processing of the Apple Pay transaction happens in the TOE Environment, on the Secure Element, using the secret card data and the Transaction Token and producing a payment cryptogram. The TOE ensures that the payment evidence transmitted back to the card issuer through the network for processing was authorized by the User (FIA\_UAU.6 Re-authenticating). In the case of Apple Pay online transactions, which are processed through the Apple Pay server, this integrity protection ensures the Dynamic Linking of the transaction data by a cryptographic based Authentication Code as exposed in the PSD2 regulation. The Apple Pay server ensures the integrity of the Dynamic Linking, and the card issuer verifies that it corresponds to a valid transaction, containing the right Transaction Token and produced by a genuine Apple Pay card (FDP\_DAU.1).

The exported user data (transaction data displayed to S.User) is controlled by FDP\_ETC.2/Transaction. The Secure Element, in the TOE Environment, is responsible for ensuring the confidentiality of the Apple Pay Card data during the transaction processing.

The following table summarizes the functions supporting Payment management.

<b>TSF</b>	<b>Description</b>
AP_Transaction	Processing of an Apple Pay transaction. <sup>5</sup>
APC_Transaction	Processing of an Apple Cash peer-to-peer transfer.

## 7.7. SF OS Update

An OS update can be offered at any time by Apple to the User. The User is required to authenticate through a passcode verification, or the update cannot be installed (FIA\_UAU.6, FIA\_UAU.2, FMT\_MTD.3).

The OS update preserves the user attributes, especially the card data, the passcode, the enrolled biometric patterns, and other authentication parameters (FIA\_ATD.1).

The ability to update the D.OS is restricted to Authenticated User (FMT\_MTD.1).

## 7.8. SF iCloud logout & Device reset

An iCloud logout is performed when the User unlinks a device from an iCloud account. When this happens, the TOE ensures that the iCloud Account related data is securely deallocated, and that no residual information is left behind (FDP\_RIP.1).

The most destructive security function available to the User on a visionOS device is the device reset, as it erases all of the User data. When this is performed, the TOE ensures that all the sensitive data terminated as part of a device reset is securely erased, leaving no residual information. This covers the iCloud Account information, all the Apple Pay Card Data, and the User authentication data such as the passcode and Biometrics (FDP\_RIP.1).

---

<sup>5</sup> Including Transfer funds with Apple Pay (refer to section 2.5.4 for details)

# Change History

Date	Version	Author	Comments
2024-12-09	1.0	Apple	Initialization of the Security Target
2025-04-03	1.1	Apple	Minor updates
2025-06-16	1.2	Apple	Minor updates