Strong Customer Authentication for Apple Pay on iPhone SE (2nd generation) with A13 Bionic running iOS 14.5.1

Security Target

Version 1.6
November 23, 2021

Apple
One Apple Park Way
Cupertino, CA 95014

Table of Contents

1. Introduction

1.1. Purpose

The purpose of this document is to define the target of evaluation for meeting the requirements of the PSD2 regulation, focusing on the Strong Customer Authentication and Dynamic Linking in Apple Pay.

1.2. Abbreviations

Abbreviation	Meaning
AP	Application Processor
API	Application Programming Interface
AR	Authorization Random
CDCVM	Consumer Device Cardholder* Verification Method
CL	Contactless
CRS	Contactless Registry Service
CVV	Card Verification Value
HSM	Hardware Security Module
I/O	Input / Output
MAC	Message Authentication Code
NFC	Near Field Communication
OS	Operating System
PNO	Payment Network Operator
PSD2	Revised Payment Service Directive Version 2
SCA	Strong Customer Authentication
SE	Secure Element
SEP	Secure Enclave
SIP	System Integrity Protection
SKS	Secure Key Store
SSE	An application in the SEP managing the pairing between the SEP and the SE
TSM	Trusted Service Manager
TSP	Token Service Provider
UID	Unique Identifier

* refers to the Apple Pay user.

2. ST Introduction

2.1. Target of Evaluation Reference

This Security Target is identified with the following information:

Security Target identifiers	
Title	Strong Customer Authentication for Apple Pay, on iPhone with A13 Bionic running iOS 14.5.1, Security Target
Version	1.6
Date	November 23, 2021
Developer	Apple Inc.

The TOE platform is an iPhone with A13 Bionic running iOS version 14.5.1, with the following platform identifiers:

Platform identifiers	
TOE	iPhone with A13 Bionic running iOS 14.5.1
Device	iPhone SE 2nd generation
Operating System	iOS 14.5.1 (Build 18E212)
Developer	Apple Inc.

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

TOE Component	Version	Description
Apple Pay App (Wallet)	App part of iOS 14.5.1	Authentication policy on data and services In-app transaction data management
Application Processor (AP)	A13 Bionic	Authentication policy on data and services In-app transaction data management
Biometric Sensor (Touch ID)	Gen 3	Sensor for fingerprint capture
Boot Loader	iOS 14.5.1 (18E212)	Allows the device to start and boot the operating system

TOE Component	Version	Description
Secure Enclave (SEP)	SEPOS part of iOS 14.5.1	Authentication Setup: Enrollment of the authentication material, User authentication verification, Authentication Prover: Passcode verification, Biometrics matching, Authentication policy on data
iOS Platform	Device operating system platform (iOS 14.5.1 (18E1212)) with the following Apple Pay services that are included in the TOE:	
• **Console**	iOS 14.5.1 (18E212)	Provides the functionality for input/output (I/O)
• **Logind**	iOS 14.5.1 (18E212)	Provides functionality for managing user logins and sessions
• **NFCd**	iOS 14.5.1 (18E212)	Provides functionality for near field communication functionality
• **Safari**	iOS 14.5.1 (18E212)	Browser
• **Settings**	iOS 14.5.1 (18E212)	Allows the user to indicate their preferred settings for the device, operating system and applications.

The Secure Element (SE) of the device is out of scope of this evaluation.

Note: *In the evaluated configuration the cryptographic modules are supplied by Apple as part of iOS and SEPOS. Readers may draw some assurance from the conformance to FIPS 140-2 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, readers should note that the browser, Safari, is evaluated for each major iOS release using the collaborative PP (cPP), Protection Profile for Application Software Version 1.3.

2.2. TOE Guidance

References to the TOE guidance document:

Apple Pay Guidance		
Strong Customer Authentication for Apple Pay on iPhone SE (2nd generation) with A13 Bionic running iOS 14.5.1: Guidance	[AGD]	Guidance, version 1.3

2.3. TOE Overview

The TOE includes the components implementing Strong Customer Authentication and Dynamic Linking in Apple Pay. The TOE is the iPhone with A13 Bionic running iOS 14.5.1 operating system. This covers the device model iPhone SE 2nd generation.

The operating system, iOS 14.5.1, manages the device hardware, provides Apple Pay and Apple Cash functionalities, and provides the technologies required to enforce Strong Customer Authentication (SCA) and Dynamic Linking for Apple Pay and Apple Cash e-commerce payments. 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.

iOS 14.5.1 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 upon user request or after a defined time of user inactivity.

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.

User authentication is provided by a user-defined passcode and 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 iOS release. Biometrics are enrolled and managed by the user. Up to 5 Touch ID fingerprints can be enrolled on a single TOE by the User.

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

The TOE relies on its environment to perform Apple Pay payments (Apple Pay transactions and Apple Cash transfers): the transaction data is always processed by the Secure Element (SE), which is outside the TOE boundary. The SE only allows a payment to be made after it receives authorization from the SEP. For each transaction, the SE utilizes the payment applets to generate a payment cryptogram. This cryptogram and the Device Account Number form a transaction-specific dynamic security code, which is provided to the payment network and the card issuer, allowing them to verify each transaction.

When interacting with Near Field Communication (NFC) compliant payment terminals, the TOE uses the device's out-of-the-TOE NFC antenna for the communication.

2.4. Description of the Apple Pay Service

2.4.1. Card provisioning

When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, the device encrypts the card information and securely sends it, along with other information about the user's account and device, through Apple Pay servers to the card issuer or the card issuer's authorized service provider. Using this information, the card issuer (or their service provider) will determine whether to approve adding the card to Apple Wallet.

Apple Pay uses three server-side calls to send and receive communication with the card issuer or network as part of the card provisioning process: Required Fields, Check Card, and Link and Provision. The card issuer or network uses these calls to verify, approve, and add cards to Apple Wallet. These client server sessions are protected for confidentiality and integrity using TLS protocol.

The full card numbers are never stored on the device or on Apple servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the SE. 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 usual credit or debit card numbers, the card issuer can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number located in the SE is isolated from the TOE, never stored on Apple servers, and never backed up to iCloud.

2.4.1.1. Adding a credit or debit card manually to Apple Pay

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 Settings, the Wallet app, or the Apple Watch app, users can enter that information by typing or using the camera on the device. When the user uses the camera to capture the card information, Apple Wallet attempts to populate the name, card number, and expiration date. The photo is never saved to the device nor stored in the photo library. When the camera is used, the user still needs to enter the CVV. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are encrypted and sent to the Apple Pay Server. 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 terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process.

2.4.1.2. Adding credit or debit cards from an iTunes Store account to Apple Pay

For a credit or debit card on file with iTunes, the user may be required to re-enter their Apple ID passcode. 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 will download and display terms and conditions, then send along the term's ID and the card security code to the Link and Provision process. Additional verification may occur for iTunes account cards on file.

2.4.1.3. 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 the card issuer's server. These keys are used to encrypt the card information that is sent to the card issuer, which prevents the information from being read by the Apple device. The provisioning flow is similar to that used for manually added cards, described previously, except one-time passwords are used in lieu of the CVV.

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

Some card issuers may also support provisioning on their websites under certain circumstances. The user can use the "Sign in with Apple" function to select an eligible device associated with their Apple ID account to provision to. The provisioning flow is similar to that used for the other methods of adding cards.

2.4.1.5. 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, or customer service call to complete the verification. For text messages or email, the user selects from contact information the issuer has on file. A code will be sent, which must be entered into Settings, the Wallet app or the Apple Watch app. For customer service, the issuer performs their own communication process.

2.4.2. Payment authorization

The SE will only allow a payment to be made after it receives authorization from the SEP. Authorization includes confirming that the user has authenticated with Touch ID or the device passcode and double-clicked the side button. Touch ID 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 a fingerprint; after five unsuccessful attempts, the passcode is required. A passcode is also required when Touch ID is not configured or not enabled for Apple Pay.

2.4.2.1. Using a shared pairing key

Communication between the SEP and the SE takes place over a serial interface, with the SE connected to the Near Field Communication (NFC) controller, which in turn is connected to the Application Processor. Although not directly connected, the SEP and the SE can communicate securely using a shared pairing key that is provisioned during the manufacturing process. The pairing key is generated inside the SEP from the device's unique identifier (UID) key and the SE's unique identifier. The pairing key is then securely transferred from the SEP to a hardware security module (HSM) in the factory, which has the key material required to then inject the pairing key into the SE. Authentication of the communication between the SEP and SE is based on AES and utilizes a MAC-specific key derived from the shared pairing key. The SEP and SE use this MAC-specific key to generate and verify the card cryptogram and host MAC to establish mutual authentication. The SEP initiates this process by sending a host challenge to the SE. The SE responds with the card challenge and card cryptogram, which the SEP uses to authenticate it. The SEP then includes a host MAC along with the transaction and authentication details as described below. The SE uses the host MAC to authenticate the SEP before continuing with processing of the transaction.

2.4.2.2. Authorizing a secure transaction

When the user authorizes a transaction, the SEP sends signed data about the type of authentication and details about the type of transaction (contactless or e-Commerce) to the SE, tied to an Authorization Random (AR) value. The AR is generated in the SEP when a user first provisions a credit card and persists while Apple Pay is enabled, protected by the SEP's encryption and anti-rollback mechanism. It is securely delivered to the SE through the pairing key. On receipt of a new AR value, the SE marks any previously added cards as deleted.

Using the pairing key and its copy of the current AR value, the SE verifies the authorization received from the SEP before retrieving encrypted payment data from a payment applet for a contactless payment. This process also applies when retrieving encrypted payment data from a payment applet for e-Commerce transactions.

2.4.2.3. 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 and/or the card issuer. Depending on the payment scheme, other data may also be used in the calculation, including:

- A Terminal Unpredictable Number, for near-field-communication (NFC) transactions
- An Apple Pay server nonce, for transactions within apps

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.

2.4.3. Paying with cards using Apple Pay

2.4.3.1. Paying with cards in stores

If the device is on and detects an NFC field, it will present the user with the requested card (if automatic selection is turned on for that card) or the default card, which is managed in Settings. The user can also go to the Wallet app and choose a card, or when the device is locked, double-click the side button on a device with Touch ID.

Next, the user must authenticate using Touch ID, or their passcode before payment information is transmitted. No payment information is sent without user authentication.

After the user authenticates, the Device Account Number and a transaction-specific dynamic security code are used when processing the payment. Neither Apple nor a user's device sends the full actual credit or debit card numbers to merchants. Apple may receive anonymous transaction information such as the approximate time and location of the transaction, which helps improve Apple Pay and other Apple products and services.

2.4.3.2. Paying with cards within apps

Apple Pay can also be used to make payments within iOS apps. When users pay within apps using Apple Pay, Apple receives the encrypted transaction information. Before that information is sent to the developer or merchant, Apple re-encrypts it with a developer-specific key. 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 iOS 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 zip 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 Touch ID or the device passcode and a double-click of the side button. After the payment is authorized, the information presented in the Apple Pay sheet will be transferred to the merchant.

2.4.3.3. App payment authorization

When the user authorizes the payment, a call is made to the Apple Pay Servers to obtain a cryptographic nonce, which is similar to the value returned by the NFC terminal used for in-store transactions. The nonce, along with other transaction data including the amount, is passed to the Secure Element to generate a payment credential that will be encrypted with an Apple key. When the encrypted payment credential comes out of the Secure Element, it's passed to the Apple Pay Servers, which decrypt the credential, verify the nonce in the credential against the nonce originally sent by the Apple Pay Servers, and reencrypt the payment credential with the merchant key associated with the Merchant ID. It's then returned 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 for processing. 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 an 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, such as an order number or customer identity, ensuring the transaction can't be diverted to a different customer. This is accomplished by the app developer, who can specify applicationData on the PKPaymentRequest. A hash of this data 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

2.4.3.4. Paying with cards at websites

Apple Pay can be used to make payments on websites with iOS devices. Apple Pay on the web requires all participating websites to register with Apple. The Apple servers perform domain name validation and issue 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 on iOS.

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

2.4.4. 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 AR value from when the card was added. This allows iOS to instruct the Secure Enclave to render cards unusable by marking its copy of the AR as invalid under the following scenarios:

- When 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

2.4.4.1. Suspending, removing, and erasing cards

Users can suspend Apple Pay on the device by placing their devices in Lost Mode using Find My iPhone. Users also have the ability to remove and erase their cards from Apple Pay using Find My iPhone, iCloud.com, or directly on their devices using the Wallet app. The ability to make payments using cards on the device will be suspended or removed from Apple Pay by the card issuer or respective payment network, even if the device is offline and not connected to a cellular or Wi-Fi network. Users can also call their card issuer to suspend or remove cards from Apple Pay.

Additionally, when a user erases the entire device—using Erase All Content and Settings, using Find My iPhone, or restoring their device—iOS will instruct the Secure Element to mark all cards as deleted. 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 ensure that all cards in the Secure Element are erased.

2.4.5. Apple Cash

Apple Pay can be used to send, receive, and request money from other users. When a user receives money, it's added to an Apple Cash account that can be accessed in the Wallet or within Settings > Wallet & Apple Pay across any of the eligible devices the user has signed in with their Apple ID.

The organizer of an iCloud family who has verified their identity 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 ID 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 our partner bank Green Dot Bank and with Apple Payments Inc., a wholly owned subsidiary created to protect your 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 trouble-shooting, fraud prevention, and regulatory purposes.

2.4.5.1. Using Apple Cash within Messages app

To use person-to-person payments and Apple Cash, a user must be signed in to 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, Messages will display 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 Wallet app.

2.4.5.2. Using Apple Cash in stores, apps, and on the web

The Apple Cash card in the Wallet app can be used with Apple Pay to make payments in stores, 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 Wallet app.

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 generate a payment signature. When the payment signature comes out of the Secure Element, it's passed 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.

If 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 ID account recovery, before regaining access to their Apple Cash balance.

2.4.6. Apple Card

2.4.6.1. Apple Card application in the Wallet app

Apple Card can be used with Apple Pay to make payments in stores, in apps, and on the web. To apply for Apple Card, the user must be signed into their iCloud account on an Apple Pay–compatible iOS or iPadOS device and have two-factor authentication set up on the iCloud account. When the application is approved, Apple Card is available in the Wallet app or within Settings > Wallet & Apple Pay across any of the eligible devices the user has signed in with their Apple ID.

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 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.

A physical card can be ordered from Apple Card in the Wallet app. After the user receives the physical card, it's activated using the NFC tag present 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 the Wallet settings. Additionally, the user can also choose to lock or unlock the physical card at any time from the Wallet app.

2.4.6.2. Apple Card payments and Apple Wallet pass details

Payments due on the Apple Card account can be made from the Wallet app in iOS 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 generate a signature. When the payment signature comes out of the Secure Element, it's passed 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.

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

2.4.7. Credit and debit cards for transit

In some cities, transit readers accept EMV (smart) cards to pay for transit rides. When users present an EMV credit or debit card to those readers, user authentication is required just as with "Paying with cards in stores."

In iOS 12.3 or later, some existing EMV credit/debit cards in the Wallet app can be enabled for Express Transit, which allows the user to pay for a trip at supported transit operators without requiring Touch ID, or a passcode. When a user provisions an EMV credit or debit card, the first card provisioned to the Wallet app is enabled for Express Transit.

The user can tap the More button on the front of the card in the Wallet app and disable Express Transit for that card by setting Express Transit Settings to None. The user can also select a different credit or debit card as their Express Transit card via the Wallet app. Touch ID, or a passcode is required to reenable or select a different card for Express Transit.

Apple Card and Apple Cash are eligible for Express Transit.

Payments with credit and debit cards for Express Transit (without requiring Touch ID, or a passcode) are not in the scope of this Security Target.

2.4.8. Express Cards with power reserve

If iOS isn't running because iPhone needs to be charged, there may still be enough power in the battery to support Express Card transactions. Supported iPhone devices automatically support this feature with the payment or transit card designated as the Express Transit card.

Pressing the side button (or on iPhone SE 2nd generation, the Home button) displays the low-battery icon as well as text indicating that Express Cards are available to use. The NFC controller performs Express Card transactions under the same conditions as when iOS is running, except that transactions are indicated only with haptic notification (no visible notification is shown). On iPhone SE 2nd generation, completed transactions may take a few seconds to appear on screen. This feature isn't available when a standard user-initiated shutdown is performed.

Payments using Express Cards with power reserve mode are not in the scope of this Security Target.

2.5. TOE Use Cases

The TOE covers the following use cases:

Use Case	Description
UC.Device_Usage	Device usage The User can manage the device's authentication credentials, including enrolling new biometric templates, updating biometric templates, deleting biometric templates and changing the passcode.
UC.OS_Update	Device Software Update 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: - No change to the User's authentication credentials (passcode or any biometrics) - No change to the User's data within the SE unless specified by the data's issuer
UC.Apple_Pay_Install_Init	Apple Pay installation and initialization The User can provision a new card in Wallet app
UC.Apple_Pay_Usage	Apple Pay usage The User can perform Apple Pay transactions.
UC.End_Of_Service	Termination by User The User can end the Apple Pay mode of operation by performing a card removal in Wallet. The User can also end all current Apple Pay services by un-registering their iCloud account. Termination by Issuer The 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.

Use Case	Description
UC.End_Of_Life	Termination of device 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.

2.6. TOE Architecture

The TOE platform includes some hardware elements of the device and all the components of the device Platform that are relevant to strong customer authentication (SCA) and Apple Pay: The SEP within the System on a Chip (SoC) of the device, and the Application Processor (AP) with the OS are the main components of this TOE. The SE is outside of the TOE boundaries.

User authentication is managed by the SEP, which defines and enforces the user access policy to data and services. The AP allows the OS to process and the OS allows the SEP to get authentication material from the various sources (biometric sensors, and the console).

iOS also allows the Apple Pay services to operate: it holds the Wallet app and relays data between the SEP and the SE

The SE is the secure component holding the Apple Pay secrets and processes the Apple Pay transactions.

This is highlighted in the following figure:

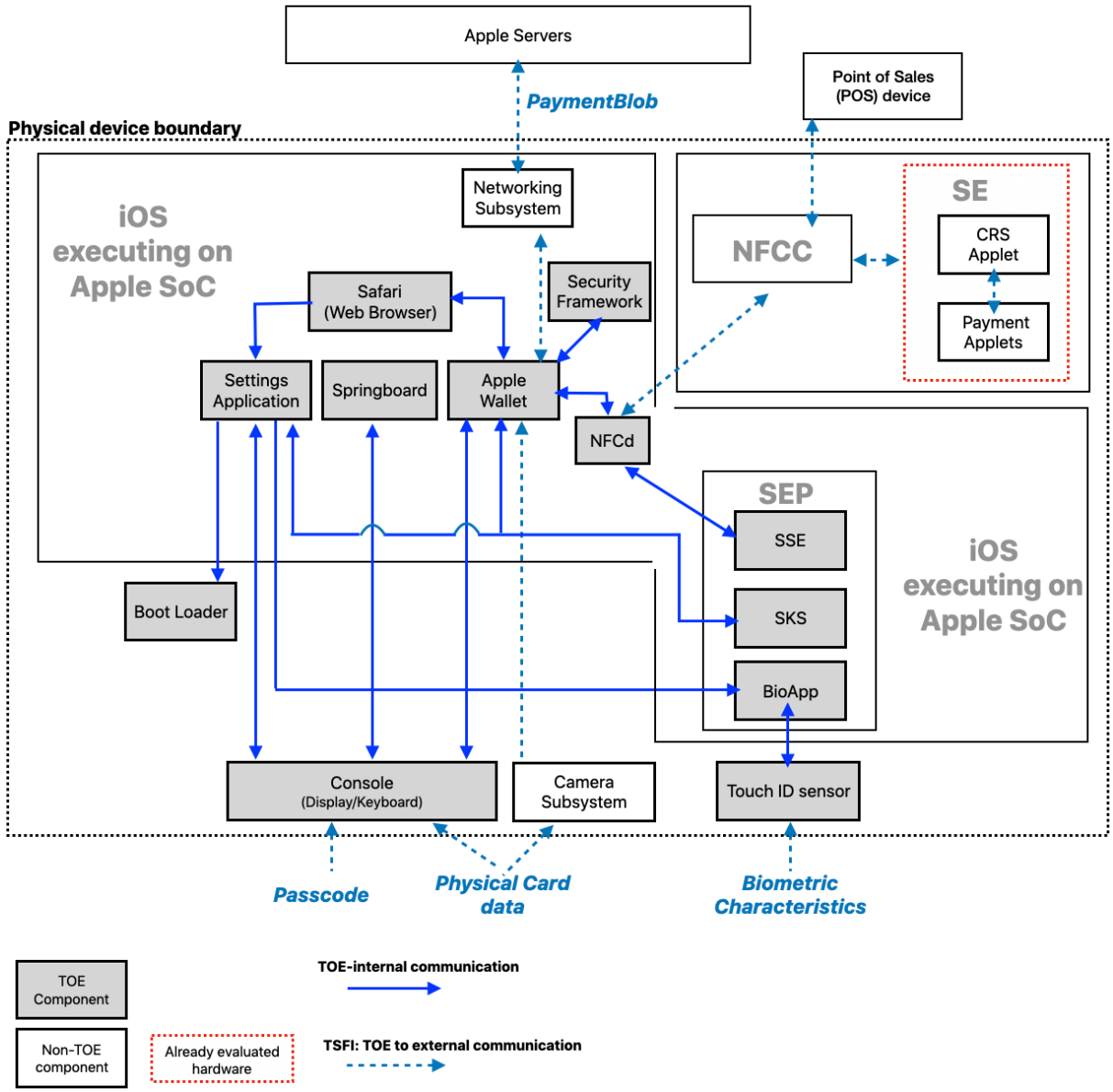

Figure 1: TOE Components and subsystems

2.6.1. TOE Environment

In this evaluation, the TOE environment includes the SE (Hardware, Operating System, CRS applet and payment applets found in the SE) and the NFC communication layer.

The SE, included in the device, is already evaluated to Common Criteria. The SE is contained in the same package as the NFCC. Payment Applets in the SE process Apple Pay transactions.

All other components and subsystems of iOS including user space and kernel software, hardware and subsystems included in the device including the camera, networking subsystems are considered part of the TOE environment. The camera is used as an input device for card data. The networking subsystem provides connectivity to the Apple Servers responsible for managing Apple Pay transactions.

2.6.2. Subsystems and Modules of the TOE

This section further breaks down the TOE components, providing more detail on the subsystems of the TOE and the modules that comprise them.

The subsystems of the TOE consist of:

- SEP: The software components of the TOE residing in the Secure Enclave (SEP). This subsystem includes several applications executing on the SEP operating system.
  - BioApp 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 (SEP) and packaged within the Application Processor.
  - The SSE (SEP-SE) manages the pairing between the SEP and the SE, allowing the SE to process only genuine and authorized Apple Pay transactions. The SSE application maintains sensitive pairing material, allowing SE and SEP to perform a mutual authentication before exchanging data.
- AW: The Wallet app subsystem handles the enrollment of applications and governs the payment operation.
- iOS components:
  - Springboard: Provides the functionality for the iOS user interface
  - NFCd: This daemon facilitates the communication between Apple Wallet and the SE
  - Safari browser: Provides the user interface to conduct payment transactions
  - Security Framework: Provides cryptographic support
  - Settings application
- Device components:
  - Touch ID sensor: The hardware component and associated drivers that allow fingerprint data to be captured and passed to BioApp to allow for enrollment and matching
  - Boot-loader: The subsystem responsible for ensuring that the device boots using software with assured integrity
  - Console: Hardware and associated drivers that handles user input via the keyboard, and displays output via the screen

All other iOS parts are outside of the TOE, including the SE together with the NFCC hardware, and the XNU iOS kernel. The iOS subsystem components are individual applications.

2.6.3. TOE Lifecycle

The TOE lifecycle phases are as follows:

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

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

The 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 organization 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 ID. 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 an iCloud account and user authentication credentials are setup (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 to the User and may involve physical destruction of the device as well as a complete reset of iOS or Apple Pay service termination by the User.

When the mobile device is received, the model of the device should be verified to verify that the model number is one of those listed in Section 2.1. This can be accomplished using any of the following methods.

- Removing the SIM tray and physically checking the upper side of the SIM tray slot
- Once authenticated to the mobile device the information is available to mobile device users in Settings » General » About, and clicking on the number displayed next to "Model"

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
Part 1: Introduction and general model	V3.1	R5	April 2017
Part 2: Security functional requirements	V3.1	R5	April 2017
Part 3: Security assurance requirements	V3.1	R5	April 2017

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	
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.3 Systematic flaw remediation
ASE: Security Target evaluation	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
	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

Assurance Class	
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

4. Security Problem Definition

4.1. Assets

The assets of this security target are:

Asset	Sensitivity*	Type	Definition
D.User_Passcode	I, C	User	Passcode value setup by the User and used to wake up device after power loss, unlock the device,and also allows the User to authorize payments (Apple Pay transactions or Apple Cash transfers).
D.User_Bio	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).
D.Card_Data	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 issuer, via Apple servers, in order to generate the Device Account Number stored in the SE.
D.User_Intent	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 payments (Apple Pay transactions or Apple Cash transfers)
D.Payment_Data	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.
D.OS	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 SEP OS), and by the User through an identified version number.
D.User_Configuration	I	TSF	User configuration is a representation of the user personal configuration including Apple Pay, Apple Cash, and Touch ID settings.
D.SEP_Configuration	I	TSF	SEP configuration is a representation of the state of the SEP in the device. It comprises (but is not limited to) the SEP OS version and the state of the user authentication functions (Passcode, enrolled biometrics, authenticated credentials, retry counters, and authentication based access control settings).
D.SEP_SE	I, C	TSF	Secret data that allows secure communication between the SEP and the SE during processing of an Apple Pay transaction or Apple Cash transfer.

Asset	Sensitivity*	Type	Definition
D.SEP_Bio	I, C	TSF	Secret data that allows secure communication between the SEP and the biometric sensor during processing of biometric authentication.

*: I = Integrity, C = Confidentiality

4.2. Subjects

The subjects of this security target are:

Subject	Definition
S.User	User of Apple Pay/Apple Cash on the device, able to: - Authenticate on the device (Biometrics or Passcode) - Manage authentication credentials (Biometrics or Passcode) - Manage device configuration (OS version, iCloud account) - Provision/enroll cards - Authorize Apple Pay transactions/Apple Cash transfers (Biometrics/Passcode and user intent) - Cancel the Apple Pay/Apple Cash service
S.Apple_Servers	Apple servers in charge of: - Management of S.User iCloud account - Management of S.User provisioning/enrollment in Apple Pay/Apple Cash - Management of OS releases, including the Wallet application - Device's interface for processing Apple Pay transactions/ Apple Cash transfers (contact S.Issuer)
S.Issuers	The Issuer or its service provider is the third party in charge of: - Management of S.User data for Apple Pay/Apple Cash services - Processing Apple Pay transactions/Apple Cash transfers
S.Merchant	The merchant is the third-party receiving payment through an Apple Pay transaction or Apple Cash transfer.
S.SE	Certified Secure Element of the device including the TOE.

4.3. Assumptions

The assumptions for this security target are the following:

Assumption	Definition
A.DEVICE_AUTH	The User of the device owns all the Apple Pay and Apple Cash activities that are performed on a device. 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.
A.PERSO	The Apple Pay and Apple Cash 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.

Assumption	Definition
A.CDCVM	The SE and its applets manage the CDCVM requirement for NFC payment transactions and require the TOE to provide user authentication and intent to pay each time CDCVM is needed. By default, applets configured for express mode do not require user authorization for transit use.

4.4. Threat Agents

The threat agents of this TOE are the following:

Threat Agent	Definition
S.Attacker	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
T.CORRUPT	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
T.PHYSICAL	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. *Note: Defending against device re-use after physical compromise is out of scope.*	D.User_Passcode D.User_Bio D.Card_Data
T.RECOVER	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 iOS erase all content and settings.	D.User_Configuration D.Card_Data D.OS
T.REPLAY	Replay	An attacker attempts to replay an Apple Pay transaction or Apple Cash transfer.	D.Payment_Data

Threat	Name	Definition	Assets
T.SILENT	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
T.SKIMMING	Authentication 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
T.USURP	Card Ownership Usurpation	An attacker could attempt to authenticate on a device, 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

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.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_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
P.UPDATE	Apple ensures that only an authenticated user can update their device's operating system to a newly released iOS. Apple also informs the Apple Pay and Apple Cash Issuers and PNOs of new applicable features of new releases.
P.DYN_LINK	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: (a) The payer is made aware of the amount of the payment transaction and of the payee; (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; (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; (d) Any change to the amount or the payee results in the invalidation of the authentication code.

5. Security Objectives

5.1. Security Objectives for the TOE

Security Objectives	Definition

OT.User_auth	The TOE enforces the following authentication policy :
	• Passcode only:
	  ○ Add, update, delete Biometrics
	  ○ Update passcode
	  ○ Modify authentication policy (except for disabling the express mode)
	  ○ Update the OS to a new version signed by Apple
	• Passcode or biometric (if enrolled)
	  ○ Unlock of the device
	  ○ Payments confirmation

OT.Card_Data	The TOE enforces that sensitive card data: • Is encrypted before being sent to the Apple servers • Is not accessible after sent to the Apple Server
OT.Passcode_Delete	The TOE enforces that removing the passcode: • Disables biometric authentication • Disables Apple Pay/Cash
OT.Card_Delete	The TOE securely triggers the delete of each individual Apple Pay/Apple Cash card when: • A card is removed from Wallet • The TOE handles the revocation of a card by its Issuer, • The use of Apple Pay is canceled (from iCloud, the Settings or passcode removal), • The iCloud account is no longer associated with the device. When a card is removed, the TOE also instructs the SE to mark it as deleted.
OT.Auth_SE	The TOE provides the SE with passcode/biometric user authentication feature for Apple Pay/Apple Cash payment/transfer approval.
OT.Payment	For eCommerce transactions and Apple Cash transfers, the TOE enforces transaction details are displayed to the User (including the card to be used from the 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 SE. For NFC transactions, if the device is on and detects an NFC field, it will present the user with the requested card (if automatic selection is turned on for that card) or the default card, which is managed in Settings. The User can also manually select a card in Wallet. The TOE also requests explicit intent from the User for Apple Pay transactions and Apple Cash transfers.
OT.Bio_Delete	TOE Biometrics delete is a secure erase of the enrolled biometric data.

Security Objectives	Definition
OT.Device_Reset	TOE securely deletes all User data when the User launches a 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.
OT.Anti_Replay	The TOE ensures that each payment processed by an Apple Pay/Apple Cash card holds the unique identifier.
OT.OS_Update	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.

5.2. Security Objectives for the environment

Environment Security Objectives	Definition
OE.Card_Data	The Issuer is responsible for using the appropriate security measures to protect the confidentiality and the integrity of the Apple Pay/Apple Cash card's sensitive data and guarantee the authenticity of card during enrolment. The SE is responsible for securing the card validation exchanges with the Issuer's TSM and for ensuring confidentiality and integrity of each Apple Pay/Apple Cash card's sensitive data during storage and use.
OE.Perso	The Issuer is responsible for verifying that the User is authorized to perform a transaction on the account of the card used as a reference, before allowing the Apple Pay/Apple Cash card personalization. The Issuer also ensures that the robustness of the personalization data, to prevent attacks like forgery, counterfeit or corruption.
OE.Card_Delete	The Issuers of all Apple Pay and Apple Cash cards installed on a device are informed when the User removes a card from that device, removes that device from the iCloud account or performs a device Erase All Content and Settings. The Issuers ensure these cards are removed from the User's account (i.e. the unlinking process of the DPAN from the FPAN, which is done by the Issuer or the corresponding TSP). The SE is responsible for securely deleting the stored Apple Pay and Apple Cash card sensitive data (private/secret).
OE.Anti_Replay	The Apple Pay server verifies that each payment (e-Commerce Apple Pay transaction or Apple Cash transfer) is not replayed. The payment is invalidated if this verification fails. For in-store transactions (i.e. NFC transactions), a similar anti-replay mechanism is used with the participation of the NFC terminal.
OE.Transaction_Verification	For Apple Pay, the cryptogram released by the SE for an Apple Pay transaction is verified before the payment proceeds. The cryptogram validation result allows the Issuer to approve or reject the transaction. The payment is invalidated if this verification fails. 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.

Environment Security Objectives	Definition
OE.Dynamic_Linking	For eCommerce transactions, the Apple Pay server preserves and Issuer verifies the cryptographic based dynamic linking of the transaction data (including amount and payee). The payment is invalidated if this verification fails.
OE.Statement	The Apple Pay card Issuers ensure that the statement associated to the card (list of transactions) is fully accurate and includes, at a minimum, the amount and recipient of each transaction. The Apple Cash card Issuer ensures that the ledger associated to an Apple Cash account (list of transfers including completed, canceled, and pending) is fully accurate.
OE.Genuine_Wallet	The Wallet application is provided and signed by Apple.
OE.CDCVM	The SE applets are responsible for checking the CDCVM state, including it within transaction data where required, and allowing normal or Express transit transactions as applicable. Payment networks or issuers are responsible for ensuring that Express transactions can only be accepted for transit specific use by requiring that non-transit Apple Pay payment transactions have a successful CDCVM.
OE.User	The S.User is responsible for ensuring that: • They own all the Apple Pay/Cash activities that are performed on a device • The passcode is robust and protected • Only their own biometrics credentials are enrolled (they do not enroll biometrics of someone else)

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
A.DEVICE_AUTH	OE.User covers A.DEVICE_AUTH ensuring the User owns and protects all the authentication credentials.
A.PERSO	OE.Perso covers A.PERSO ensuring the provisioning process verifies the ownership of the provisioned cards.
A.CDCVM	OE.CDCVM covers A.CDCVM ensuring the SE uses the TSF features when required.
T.SKIMMING	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 application 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
T.USURP	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 SE. 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. OT.User_Auth and OE.Genuine_Wallet additionally ensure that the installation of a new Apple released OS or Apple Wallet application preserves the confidentiality and integrity of the payment data. OT.Passcode_Delete ensures that if passcode login is disabled, the Apple Pay and Biometric authentication are not available anymore.
T.RECOVER	OT.Bio_Delete ensures that a removed passcode or biometric credential cannot be recovered. OT.Card_Data, OT.OS_Update and OE.Card_Data ensure that the confidential card data are only stored by the SE which protects them from disclosure. OT.Device_Reset covers the physical erase of the content and settings of the device where the TOE will trigger secure erase all Apple Pay card data. OE.Card_Delete ensures that the Issuers of Apple Pay cards are securely removing the deleted cards from the User's account so that no transaction can further proceed.
T.REPLAY	OE.Anti_Replay ensures that each Apple Pay transaction or Apple Cash transfer is not replayed. OE.Anti_Replay and OT.Anti_Replay ensures that each Apple Pay transaction or Apple Cash transfer cannot be replayed.
T.CORRUPT	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 by the Apple Pay 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 Issuer ensures that all processed Apple Pay transactions appear on the statement of the account associated to the card. OT.User_Auth and OE_Genuine_Wallet ensure that the Apple release of a new OS or Apple Wallet application implementing the payment functions are controlled.
T.SILENT	OT.User_Auth and OT.Payment ensure that an Apple Pay transaction or Apple Cash transfer is always authorized by the User. 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. OT.User_Auth and OE.Genuine_Wallet ensure that the Apple release of a new OS or Apple Wallet application implementing the authentication functions and payment functions is controlled. OT.Passcode_Delete ensures that if passcode is turned off, the Apple Pay and Biometric authentication are not available anymore.

Element	Rationale
T.PHYSICAL	The User credentials maintained by the TOE are secured by OT.User_Auth enforcing the secure verification process of Biometrics or Passcode. 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. OT.Card_Data, OT.OS_Update and OE.Card_Data ensure that the Apple Pay/Apple Cash card data is kept confidential in the SE and cannot be extracted.
P.UPDATE	OT.User_Auth and OE.Genuine_Wallet ensure that the Apple release of a new OS or Apple Wallet application implementing the authentication functions and payment functions are controlled, and that it preserves the confidentiality and integrity of the authentication and payment data.
P.DYN_LINK (Dynamic Linking)	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: **(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. **(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), OE.Anti_Replay ensures that each payment is uniquely identified, and OT.Payment ensures that the payment data is integrity protected. **(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. **(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.

Security Objectives mapping table:

	T.CORRUPT	T.PHYSICAL	T.RECOVER	T.REPLAY	T.SILENT	T.SKIMMING	T.USURP	P.DYN_LINK	P.UPDATE	A.PERSO	A.DEVICE_AUTH	A.CDCVM
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			
OT.Passcode_Delete						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.CDCVM												x
OE.User							x				x	
OE.Genuine_Wallet	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:

Authentication_SFP	Authentication policy enforcing authentication, re-authentication and authorization rules as defined by OT.User_Auth. This SFP includes information flows between the SEP and the biometric sensor (for biometric authentication).
Payment_SFP	Security policy enforcing that processing 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 their exportation.
Card_Perso_SFP	Security policy enforcing that: - Importing D.Card_Data is only allowed if a passcode is configured - Confidential parts of the card data are protected before being sent to the Apple Servers - Confidential parts of the card data are not imported in the Wallet

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		
Card Data Confidential parts	Parts of the Card Data that should stay confidential and not been stored in the Wallet	- Secret parts of the card number - CVV - …
User Authorization	Part of D.Payment_Data specifying the explicit authorization of the S.User	- "yes" - "no"
Erase Data	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.	- "enabled" - "disabled" (default)
BioAuth Unlock	Part of D.User_Configuration, authorization to use biometric authentication for unlocking a locked device, "selected" or "not selected" by the User.	- "selected" - "not selected" (default)
BioAuth AP	Part of D.User_Configuration, authorization to use biometric authentication for Apple Pay operations, "selected" or "not selected" by the User.	- "selected" (default) - "not selected"
Apple OS public key	The public key used to check the authenticity of a new version of D.OS.	- Part of installed D.OS
OS_signature	Part of the OS file that is checked by the TOE before updating D.OS	- Part of the update file

Security Attribute		
Passcode_off	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.	- "disabled" (default) - "enable"

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 *passcode authentication, biometric authentication (*fingerprint*)* to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the: • *Passcode authentication as default authentication* • *Biometric authentication for:* - *unlock if selected in the "Touch ID & Passcode" configuration (BioAuth Unlock = selected)* - *transaction authorization if selected in the "Touch ID & Passcode" configuration (BioAuth AP = selected)* • *Rules defined in FIA_UAU.6 Re-authenticating and FIA_AFL.1 (Biometric/Erase/Delay) Authentication failure handling*.

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 *Biometric validation*.
FIA_AFL.1.2 /Biometric	When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall *require Passcode validation, blocking further Biometric validation attempts*.

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 *passcode validation*.
FIA_AFL.1.2 /Erase	When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall *erase data on iPhone if "Erase Data" = enable*.

FIA_AFL.1/Delay Authentication failure handling

FIA_AFL.1.1 /Delay	The TSF shall detect when *5 (five)* unsuccessful authentication attempts occur related to *passcode validation*.
FIA_AFL.1.2 /Delay	When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall *start delaying further passcode validation attempts and require passcode validation*.

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1	The TSF shall re-authenticate the user under the conditions *that the user requests:* • *OS update (change of D.OS)* • *"Touch ID & Passcode" configuration change (once for all "Touch ID & Passcode" parameters until "Touch ID & Passcode" interface is closed), including "BioAuth Unlock" and "BioAuth AP", passcode and Biometric patterns* • *Transaction validation (export of D.Transaction_Data), the re-authentication should be done during the 60 seconds after the transaction validation request*.

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 *D.Payment_Data (including S.Merchant and S.User data)*.
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: *D.User_Passcode, D.User_Bio, D.Card_Data, BioAuth Unlock, BioAuth AP*.
Refinement: The update of D.OS shall not modify these user attributes.	

6.3. Access/Flow Control SFRs

6.3.1. Authentication _SFP

FDP_ACC.2/Authentication_SFP Complete access control

FDP_ACC.2.1/ Authentication_SFP	The TSF shall enforce the *Authentication_SFP* on*:* Subjects: *S.User* Objects: *the TSF* and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2/ Authentication_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 *Authentication_SFP* to objects based on the following: Subjects: *S.User* Objects: *the TSF* Security attributes: *none*
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: *S.User is authenticated according to FIA_UAU.5*
FDP_ACF.1.3/ Authentication_SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.
FDP_ACF.1.4/ Authentication_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *"Passcode_off" is enabled*.

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1	The TSF shall enforce the *Authentication_SFP* to prevent the *modification and disclosure 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 SEP. Protection against modification includes also 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 *Payment_SFP* 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: - *exported Payment_SFP details (the card to be used from the 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)* - *D.Payment_Data includes a unique identifier, which can be either:* - *A Terminal Unpredictable Number, for near-field-communication (NFC) transactions, or* - *An Apple Pay server nonce, for transactions within apps or Apple Cash transfers.*

FDP_ACC.2/Payment_SFP Complete access control

FDP_ACC.2.1/ Payment_SFP	The TSF shall enforce the *Payment_SFP* on: Subjects: *S.User* Objects: *D.Payment_Data (including S.User and S.Merchant Data)* and all operations among subjects and objects covered by the SFP.
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 SE.

FDP_ACF.1/Payment_SFP Security attribute based access control

FDP_ACF.1.1/ Payment_SFP	The TSF shall enforce the *Payment_SFP* to objects based on the following: Subjects: *S.User* Objects: *D.Payment_Data (including S.User and S.Merchant Data), the SE (through a trusted channel)* Security attributes: *"User Authorization", "BioAuth AP", "Passcode_off"*
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: - *Export of D.Payment_Data with "User Authorization" set to "yes" to the SE is allowed if:* - *S.User shows their intent to pay (using the gesture of activating the Touch ID sensor combined with successfully matching the user's fingerprint)* - *S.User had been successfully re-authenticated for transaction validation (FIA_UAU.6)*.
FDP_ACF.1.3/ Payment_SFP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.
FDP_ACF.1.4/ Payment_SFP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *"Passcode_off" is "enabled"*.

6.3.3. Card_Perso_SFP

FDP_ACC.2/Card_Perso_SFP Complete access control

FDP_ACC.2.1 /Card_Perso_SFP	The TSF shall enforce the *Card_Perso_SFP* on Subjects: *S.User, S.Apple_Servers* Objects: *D.Card_Data* and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2 /Card_Perso_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/Card_Perso_SFP Security attribute based access control

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

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 *Card_Perso_SFP* 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: - *D.Card_*Data *is encrypted before being exported to S.Apple_Server* - *"Card Data Confidential parts" are not kept on the TOE after being exported*.

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/Card_Perso_SFP Import of user data without security attributes

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

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. SEP/SE 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 *the TSF* to initiate communication via the trusted channel.
FTP_ITC.1.3/SE	The TSF shall initiate communication via the trusted channel for *Payment initiation and transmission of D.Payment_Data*.

FDP_UCT.1/SE Basic data exchange confidentiality

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

FPT_RPL.1/SE Replay detection

FPT_RPL.1.1/SE	The TSF shall detect replay for the following entities: *S.SE*.

FPT_RPL.1.2/SE	The TSF shall perform *reject data* when replay is detected.

6.5. Local data protection

FPR_UNO.1 Unobservability

FPR_UNO.1.1	The TSF shall ensure that *S.Attacker* are unable to observe the operation *Passcode set, Passcode check, Passcode Update, Passcode removal, Biometrics set, Biometrics check, Biometrics update, Biometrics delete, Apple Pay/Cash Card provisioning,* on *D.User_Bio, D.User_Passcode, D.Card_Data* by *S.User*.

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 *deallocation of the resource from* the following objects: *D.User_Bio, D.User_Passcode, "Card Data Confidential parts" and iCloud Account (in D.User_Configuration)*.
Refinement: • The removal of the iCloud Account by the S.User triggers the deallocation of all the Apple Pay data/configuration. • The revocation of individual card by its issuer triggers the deallocation of the related card data. • The procedure of Reset on the device triggers the deallocation of all security attributes except the D.OS. • The removal of "Card Data Confidential parts" is done by instructing the SE to mark the card as deleted. • The removal of the Passcode by the S.User disables the actual Passcode; and triggers the deallocation of the iCloud Account information and all the Apple Pay data.	

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 *integrity errors* on all objects, based on the following attributes: *D.User_Bio, D.Card_Data, D.OS*.

6.6. TSF management

6.6.1. Roles and Management Functions

FMT_SMR.1 Security roles

FMT_SMR.1.1	The TSF shall maintain the roles *Authenticated User*.
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: *management of security attributes (see FMT_MSA.1)*.

6.6.2. Management of security attributes

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1	The TSF shall enforce the *Payment_SFP, Card_Perso_SFP* to provide ***"BioAuth Unlock"*** restrictive (disabled) ***"BioAuth AP"*** permissive (selected) ***"Passcode_off"*** restrictive (disabled) ***"Erase Data"*** permissive (disabled) default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow *nobody* 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 *Authentication_SFP, Card_Perso_SFP* to restrict the ability to *modify* the security attributes ", *"BioAuth Unlock", "BioAuth AP", "Passcode_off", "Erase Data"* to *"Authenticated User"*
Refinement: • When "Passcode_off" is enabled, the TSF removes the D.Card_Data according to FDP_RIP.1.	

6.6.3. Management of TSF_Data

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1	The TSF shall restrict the ability to *update* the *D.OS* to "*Authenticated user"*.

FMT_MTD.3 Secure TSF data

FMT_MTD.3.1	The TSF shall ensure that only secure values are accepted for *D.OS*.
Refinement: secure value is defined by "OS_signature" is valid and signed by "Apple OS public key".	

6.7. Security Requirements Rationale

6.7.1. Security Functional Requirements (SFR) Dependencies

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

Requirements without dependency: FIA_UID.2, FIA_UAU.6, FIA_UAU.5, FDP_DAU.1, FIA_ATD.1, FPT_ITC.1, FTP_ITC.1/SE, FPT_RPL.1/SE, FPR_UNO.1, FDP_RIP.1, FMT_SMF.1 and FDP_SDI.1

6.7.2. Rationale SFR/Security Objectives for the TOE

Objective reference	Rationale
OT.User_Auth	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. FIA_UAU.5 specifies different authentication methods. 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. 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. FIA_ATD.1, FMT_MSA.3, FMT_MSA.1 and FMT_MTD.1 specify the management of related information. FMT_MTD.3 specifies the signature verification on the OS update. FIA_AFL.1 (Biometric/Erase/Delay) specify the failure handling in case of wrong biometric or passcode authentication. FDP_ITT.1 also support this objective ensuring the biometric data is not modified or disclosed during internal transfer.
OT.Card_Data	The SFP Card_Perso_SFP and the associated SFRs (FDP_ACC.2/Card_Perso_SFP, FDP_ACF.1/Card_Perso_SFP, FDP_ITC.1/Card_Perso_SFP and FDP_ETC.2/Card_Perso_SFP, FPT_ITC.1) enforce card data stored in the wallet does not include sensitive card data as this one is only sent to the SE. FTP_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. FPR_UNO.1 ensures the non-observability of secret card data. FDP_SDI.1 ensures card data stored in containers controlled by the TSF are monitored for integrity errors.
OT.Passcode_Delete	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. FIA_UAU.6 enforces a re-authentication for changing the Passcode_off configuration. FPR_UNO.1 ensures the non-observability of the passcode.
OT.Card_Delete	FDP_RIP.1 ensures the confidential parts of the card data are securely removed by the SE. Refinement of FMT_MSA.1.1 ensures the secure delete in case of passcode turning off. FPR_UNO.1 ensures the non-observability of sensitive card data.
OT.Auth_SE	FIA_UID.2, FIA_UAU.2, FIA_UAU.5 specify the base of the authentication feature. FIA_AFL.1/Biometric enhance the biometric security limiting the authentication attempts before requiring passcode authentication. Other FIA_AFL.1 protect the TSF and the user data against brute force attacks. FIA_UAU.6 specifies the re-authentication for some functions of the TOE.

Objective reference	Rationale
OT.Payment	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 evidences of the validity of Apple Pay Transaction Data, verifiable by the Issuer. FDP_ACC.2/Payment_SFP and FDP_ACF.2/Payment_SFP ensure user authorization is done before each transaction. FPT_RPL.1/SE ensures transaction replay detection.
OT.Bio_Delete	FDP_RIP.1 ensures biometric data delete is a secure erase.
OT.Device_Reset	FDP_RIP.1 ensures all sensitive data are securely removed during a device reset
OT.Anti_Replay	FDP_ETC.2.4/Transaction ensures a unique identifier provided by the NFC terminal or Apple server is included in the transaction data, avoiding any replay attack.
OT.OS_Update	FIA_UAU.6.1 ensures S.User is re-authenticated before the OS update proceeds. The refinement of 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.

6.7.3. SAR Dependencies

TOE SAR	Dependencies
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1
ADV_FSP.3	ADV_TDS.1
ADV_TDS.1	ADV_FSP.2
AGD_OPE.1	ADV_FSP.1
AGD_PRE.1	No dependencies
ALC_CMC.2	ALC_CMS.1
ALC_CMS.2	No dependencies
ALC_DEL.1	No dependencies
ALC_FLR.3	No dependencies
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1
ASE_ECD.1	No dependencies
ASE_INT.1	No dependencies
ASE_OBJ.2	ASE_SPD.1
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1
ASE_SPD.1	No dependencies
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1
ATE_COV.1	ADV_FSP.2, ATE_FUN.1
ATE_FUN.1	ATE_COV.1
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1

TOE SAR	Dependencies
AVA_VAN.2	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1

All the dependencies are covered.

6.7.4. 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 attacker 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 Touch ID as a Biometric authentication method, the device must be set up so that a passcode is required to unlock it.

Touch ID is Apple's fingerprint authentication system that enables secure access to an iPhone equipped with the Touch ID sensor.

When Touch ID detects a successful match, the device unlocks without asking for the device passcode. Touch ID does not replace the passcode but provides easy access to the device within defined boundaries and time constraints. To use Touch 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
- 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
- The device has received a remote lock command
- The User exited power off/Emergency SOS by pressing and holding either volume button and the Sleep/Wake button simultaneously for 2 seconds and then pressing Cancel
- 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)

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 and FMT_MSA.1 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 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 a Biometrics.
	Bio_Delete: Delete an enrolled Biometrics credential (one, or all).

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: first unlock after power-on or reboot,

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 Passcode or any other activated (with enrolled templates) authentication method to perform unlock (beyond first unlock), 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 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 were to use this path for attempting an observation-based attack (FPR_UNO.1).

The SE, 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 Touch ID service. To use Touch 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 fingerprint 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). A User can enroll up to 5 fingerprints for Touch ID.

7.1.6. Bio_Update

Once a fingerprint is enrolled on a device, the User can update it within the settings of the Touch 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 Touch ID, deleting the associated templates, and re-enroll their fingerprint 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 Biometrics 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. SF.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 Touch ID settings on the device, using the Reset Touch ID option. This function deletes the associated template of all the fingerprints enrolled. This function, like the others, 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).

7.2. SF Biometric/SEP secure channel

The TSF protects the data exchanged between the biometric sensor and the Secure Enclave Processor against disclosure and modification (FDP_ITT.1)

7.3. SF SEP/SE secure channel

The TSF is able to initialize a secure channel with the SE (FTP_ITC.1/SE). This secure channel protects the exchanged data with its corresponding security property: against disclosure (FDP_UCT.1/SE), modification (FDP_UIT.1/SE) and replay (FPT_RPL.1/SE).

7.4. 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: Issuer initiated suspend/unlink of an Apple Pay Card in 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: Issuer initiated suspend/unlink of user's Apple Cash services.

7.4.1.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)

The first three modes are only available to an authenticated User on the device, with passcode enabled (FIA_UAU.2, FDP_ACC.2/Card_Perso_SFP, and FDP_ACF.1/Card_Perso_SFP).

When a User adds a card to 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/Card_Perso_SFP) or on Apple servers.

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

7.4.2.AP_Cancellation

When the User decides to remove an Apple Pay card from the Apple Wallet, the TSF order the SE to securely invalidate and remove the Device Account Number (FDP_RIP.1).

7.4.3.AP_Revocation

When the Issuer decides to suspend or unlink an Apple Pay card from the Apple Wallet of a TOE User, the TSF order the SE to securely invalidate and remove the Device Account Number (FDP_RIP.1).

7.4.4.APC_Card_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/Card_Perso_SFP) 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)

7.4.5. APC_Disenroll

When the User decides to remove an Apple Cash card from the Apple Wallet, the TSF order the SE to securely invalidate and remove the Device Account Number (FDP_RIP.1).

7.4.6. APC_Revocation

When the Issuer decides to suspend or unlink an Apple Cash card from the Apple Wallet of a TOE User, the TSF order the SE to securely invalidate and remove the Device Account Number (FDP_RIP.1).

7.5. SF Payment management

When a device initiates an Apple Pay transaction, the SE, in the TOE Environment, only allows a payment to be made after it receives authorization from the SEP. 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).

Apple Pay includes an anti-replay mechanism that prevents transactions to be repeated by including in D.Payment_Data:

- A Terminal Unpredictable Number, for near-field-communication (NFC) transactions, or
- An Apple Pay server nonce, for transactions within apps or on the web

The processing of the Apple Pay transaction happens in the TOE Environment, on the SE, using the secret card data, the Transaction Token and producing a payment cryptogram. The TOE ensures that the payment evidence transmitted back to the Issuer for processing (through a Terminal or network) 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 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 SE, 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.

TSF	Description
AP_Transaction	Processing of an Apple Pay transaction.
APC_Transaction	Processing of an Apple Cash peer-to-peer transfer.

7.6. 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).

7.7. 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 an iOS device is the device reset, as it erases of all the User data. When this is performed, the TOE ensures that all the sensitive data deallocated as part of a Device Reset is protected from leaving residual information. This covers the iCloud Account information, all the Apple Pay Card Data, and the User authentication data like passcode and Biometrics (FDP_RIP.1).

Change History

Date	Version	Author	Comments
2021-07-27	1.3	Apple	New edition of Security Target
2021-08-20	1.4	Apple	Minor fixes
2021-10-20	1.5	Apple	Updates according to internal reviews
2021-11-23	1.6	Apple	Front page modification

