VeroGuard HSM Digital ID Security Target

ST Date: 03 February 2022

ST Version: 1.19

1 Document Introduction

This document is the Common Criteria Security Target for “VeroGuard HSM Digital ID for Open Networks”. It defines all the elements of a Common Criteria Security Target as defined in Common Criteria Version 3.1 Revision 5 Part 1, Part 2, and Part 3.

2 Revision History

Version	Date	Notes
0.1	05 August 2020	First Draft
0.2	13 August 2020	Internal review version
0.3	14 August 2020	Draft release to VeroGuard
0.4	23 September 2020	Abbreviation changed to Acronyms. Heading and subheadings.
0.5	22 November 2020	After delivery of requested API documentation
0.6	24 November 2020	Post-review changes.
0.7	25 November 2020	After stakeholder meeting
0.8	01 December 2020	Review and update claims, replace TOE with VeroCard in selected places
0.9	02 December 2020	Reference ALC_DEL preparatory statement v0.5
0.10	03 December 2020	Requested changes and images incorporated
0.11	10 December 2020	Updated tables 3 and 5, Open ID Connect details added
1.0	13 January 2021	Work in Progress after initial review
1.1	08 February 2021	After requested changes and reformatting
1.2	09 February 2021	After review and changes to non-TOE listing
1.3	10 February 2021	Document Review. Comments stripped and changes accepted. Some spacing added.
1.4	14 February 2021	Updated after comments on section 14.1.3
1.5	18 March 2021	Sections 8, 9 updated to include security problem statement
1.6	6 April 2021	Revised threats, OSPs and assumptions with rationale. Modified Sections 12, 14 and 15 according to additional input from VeroGuard. Performed a full document review.
1.7	8 April 2021	Additional input regarding section 15.3. Rooting out inconsistencies in tables 1 and 2. Added more acronyms.

1.8	27 April 2021	TOE Name changed. After evaluator cursory review and suggestions
1.9	03 June 2021	Updated version numbers of TOE components. Removed section 9.4 TOE Application Lifecycle Delivery Document. Added this data to references section Removed section 9.5 TOE Application Guidance Documents. Added this data to references section Added mapping security objectives of TOE components in section 9.3 to security objectives in section 12.1 Updated various sections in response to ACA comments
1.10	02 July 2021	This version was created in response to ST EOR 01 Table 1, date row removed References to production DocuSign HSM were added in Sections 9.3.7. and 10.3 S 12.3.1.4 Removed reference to HSM S13, 14 updated
1.11	09 July 2021	After EOR response and review
1.12	03 August 2021	TOE Component versions in table 3 reviewed All references to SDKMod were changed to “VeroGuard SDKMod custom component” FPT_TST.1.2 “data Integrity” was removed.
1.13	12 October 2021	VeroCard Hardware version erratum was addressed. Correct hardware version is VK30D-0001. Section 9.3.6 Added qualification to firmware upgrades. Section 14.1.2 FDP_ACF.1.3. Reference to being able to authorise firmware upgrade was removed Section 8.3 VeroGuard.Tms.exe version was changed to 1.0.860.1
1.14	25 November 2021	Section 8.3 Table 3 TOE Component VeroGuard.HSM.Host.DLL version number changed to 1.0.860.2 in accordance with VeroGuard website. This version has TLS1.2 for the production HSM enabled.

		Table 6 and 7 T_Physical_Tempering was changed to T.PHYSICAL_TAMPERING. S 12.3.1.8 T_EAVES_P changed to T.EAVES_P
1.15	30 November 2021	S 14.3.2 Table 10 OPHYSICAL_INTEGRITY changed to O.PHYSICAL_INTEGRITY. S 14.1 and 14.3 Table 9 reference to FCS_COP.1.1/ECDH256 removed. S 14.3 FMT_SMR.1 and FIA_UID.1 were added to tables 9 and 10. S 15.7 Justification of these SFRs was added
1.16	15 December 2021	S 10.2 Table of claims specific to VeroCard was edited to remove one claim and the validation column as these were considered no longer relevant. S 14.1.4 FDP_ACF.1.3 and FMT_SMR.1 were updated to reflect the list of roles in ADG_CC_001 VeroGuard Digital ID Solution Admin Guide sections 8.3 to 8.5
1.17	23 December 2021	S 8.1 Table 1 references updated to version 1.17 and to include “VeroGuard HSM Digital ID” S 9.1.2 section title changed to “Windows 10 Credential **Management** Vulnerability”. S 12.1 Table 7 T.UNEXPECTED_BEHAVIOUR was added to the table in accordance with S 11.1.6. Sections 12.2 updated to reference OSP. Referenced OSPs were then added to table 6 for O.DATA_INTEGRITY. Reference list item PCI PTS POI Technical FAQ removed. Other references were updated to reflect renamed developer delivered references. VeroGuard Digital ID changed to VeroGuard HSM Digital ID for Open Networks in various places. Sections 12.3.1.14 to 12.3.1.16 added to rationale of security objectives. Headings for sections 11, 12, 12.1, 12.2 changed from APE_ to ASE_
1.18	11 January 2022	In response to EOR 09 (ID: 4), S14.1.2 added referenced to FDP_ITC.2.5 S 14.1.6 updated FTP_ITC.1.2 and FTP_ITC.1.3 updated to reference secure communication functions
1.19	03 February 2022	S3 Acronyms added RBAC and VMS. Added text in footer “For public release” In response to ACA comments:

		S8.2 Table 2 version of Admin Guide document version number added. S10 conformance claim wording changed. S12.2.6 O.PIN_PROTECTION rationale changed from FCS_COP.1.1/AES to FCS_COP.1.1/SHA-256. Table 10 updated S12.3 updated to document rational for mapping security objectives (O) to SFRs. Table 7 updated to reflect S12.3.1.4. Table 8 updated to reflect S12.3.2.5 S14.3.2 rationales updated to reflect table S15 SFRs added to reference FDP_RIP.1.1/Keyloader, FPT_ITC.1 and FPT_TDC.1 Header text for section 2 onwards changed to ""VeroGuard HSM Digital ID for Open Networks"

3 Acronyms

Initial	Abbreviation
AD	Active Directory
ANSI	American National Standards Institute
API	Application Programming Interface
BDK ID	DUKPT Base Derivation Key (BDK) ID
BLE	Bluetooth Low Energy
BoID	Bureau of ID
CBC	Cypher Block Chaining
CC	Common Criteria
CPU	Central Processing Unit
DPA	Differential Power Analysis
DUKPT	Derived Unique Key Per Transaction
DNS	Domain Name System
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards
GPS	Global Positioning Service
HSM	Hardware Security module
IC	Integrated Circuit
ID	Identity
IEC	International Electrotechnical Commission
IIS	Internet Information Server
IPEK	Initial PIN Encryption Key
KEK	Key Encryption Key
MAC	Message Authentication Code or Media Access Control

MFA	Multi-Factor Authentication
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OS	Operating System
OSP	Organizational Security Policy
PAN	Primary Account Number
PC	Personal Computer
PCB	Printed Circuit Board
PED	PIN Entry Device (VeroCard ID)
PEK	PIN Encryption Key
PIN	Personal Identification Number
POI	Point of Interaction
POS	Point of Sale (a kind of POI)
RAND	Random Number
RBAC	Roles Based Access Control
RFID	Radio Frequency Identification
RKI	Remote Key Injection
RNG	Random Number Generator
SDK	Software Development Kit
SFP	Security Function Policy
SFR	Security Functional Requirement
SPA	Simple Power Analysis
ST	Security Target
STS	Security Token Service
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

TSS	TOE Summary Specification
VGS	VeroGuard
VMS	VeroGuard Manufacturing System

4 References

[CC Part1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model. April 2017 Version 3.1 Revision 5 CCMB-2017-04-001.

[CC Part 2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components. April 2017 Version 3.1 Revision 5 CCMB-2017-04-002.

[CC Part 3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components. April 2017 Version 3.1 Revision 5 CCMB-2017-04-003.

ADG_CC_001 VeroGuard HSM Digital ID Solution Admin Guide version 2.2

POL_CC_001 VeroCard Security Policy

SPC_CC_004 VeroCard Key Loading Design & Implementation

USG_CC_001 VeroCard User Guide

T091-500-004-ALC_DEL.1 Application Lifecycle Delivery

T091-500-005-AGD_OPE.1 Guidance Operation

PCI PTS POI Modular Security Requirements version 5.1

NIST Cryptographic Module Validation Program

NIST SP 800-121 Guide to Bluetooth Security

Launch Studio Bluetooth declared products list

DocuSign 5.0 Security Policy Document 140sp2860

5 Table of Contents

6 Table of Figures

7 Tables

8 Security Target (ST) Introduction (ASE_INT)

This section is the Security Target Introduction. The following topics are described:

- ST Reference
- ST and Target of Evaluation (TOE) Descriptions
- Components of the TOE; and
- Non-TOE Components

8.1 ST Reference

This section describes the ST.

ASE_INT Item	ST Value
ST Title	VeroGuard HSM Digital ID Security Target
ST Version Number	1.19
ST Reference	VeroGuard_HSM_Digital_ID_ST_EAL2+_v1.19

Table 1 Security Target (ST) Reference

8.2 TOE Reference

Information that describes TOE appears in the table below:

ASE_INT Item	ST Value
Product Name	VeroGuard HSM Digital ID for Open Networks
TOE Type	ICs, Smart Cards and Smart Card-Related Devices and Systems
Version	1.0
Date	8 April 2021
Guidance	ADG_CC_001 VeroGuard HSM Digital ID Solution Admin Guide v2.2

Table 2: TOE Reference

8.3 Components of TOE

This section describes the defining components of the TOE and their version numbers. Version numbers listed in this section describe the TOE in the configuration presented for evaluation.

The defining hardware elements of the TOE are:

- VeroCard version VK30D-0001; and
- DocuSign HSM hardware version 5.0.

The following components are required for operation of the TOE in the evaluated configuration. Note: For software versions, claims are relevant to the Major and Minor revision numbers only. See the Application Lifecycle Delivery (ALC_DEL) Preparatory Statement for guidance on software version numbers. The defining executable components of the TOE are listed in the table below:

TOE Component	Version	Supporting Element
Keyloader	1.0.26	VeroGuard Manufacturing System
VeroCard Firmware including Bluetooth driver	VC0001xxxxxx	VeroCard version VK30D-0001
DocuSign HSM Firmware	5.0.2	DocuSign HSM hardware version 5.0
Serenity Credential Provider	1.0.107.0	Windows 10 (see Serenity Login Installer)
VeroGuard.Tms.exe	1.0.860.1	Windows 2016 Server or later
VeroBureau.Api.exe	1.3.148.1	Windows 2016 Server or later with IIS 7.5 or later
VeroGuard.Terminal.Activate.Host.dll	1.0.860.0	
VeroGuard.Card.Service.exe	1.0.64.0	
VeroGuard.Hsm.Host.dll	1.0.860.2	
VeroGuard.Terminal.Host.dll	1.0.860.0	
VeroGuard SDKMod Custom Component	1.0.0	Production DocuSign HSM

Table 3: Software and Firmware Components of TOE

Security Objectives of the TOE components are described in section 9.3.

8.4 Non-TOE Components

This section lists the Non-TOE components.

8.4.1 Server Applications including Open ID Connect with OAuth2

Windows Active Directory and the Open ID Connect (OAuth2) implementation are not part of the TOE. The Open ID Connect implementation authenticates communication between the VeroGuard.Terminal.Host.dll API (client) and VeroBureau.API.exe (server). The “Open ID Connect with OAuth2” implementation authorises but does not authenticate communication between the web browser and other applications. Open ID Connect with OAuth2 depends on an Open LDAP database which is hosted on an Ubuntu Linux operating system.

8.4.2 Web Browsers

Web browsers that implement ECMAScript 6 support Bluetooth communication. This feature enables the TOE to authenticate the VeroCard but is not considered part of the TOE.

8.4.3 Operating Systems and Generic ICT Hardware

Microsoft Windows or other operating systems, communication devices such as switches and cables are not considered part of the TOE.

8.4.4 Windows Drivers

The Windows Bluetooth driver and the web browser are not part of the TOE. This is not to be confused with the VeroCard Bluetooth driver which is part of the VeroCard executable.

9 TOE Overview

This section describes:

- Security Problem and Use Cases
- Introduction to the TOE
- Security Objectives of the TOE Components
- Physical Scope of the TOE; and
- Non-TOE components

9.1 The Security Problem

This section describes security concerns that the TOE claims to address:

- Web Application Credential Management Vulnerability
- Windows 10 Credential Management Vulnerability; and
- Use of personal electronic devices for MFA in Secure Environments

These security problems are considered as use cases for credential management for web applications, credential management for Windows Active Directory and general multi-factor authentication (MFA) without an authorisation component.

9.1.1 Web Application Credential Management Vulnerability

When a user enters a username and password into a web application, the authentication request is sent using the default encryption of the web site. The TOE described in this document solves the problem described above by integrating with IdentityServer4 Open ID Connect with OAuth2. When the TOE is used with IdentityServer4 Open ID Connect and OAuth2, the combination protects against these vulnerabilities:

- Phishing
- Credential stuffing
- Brute Force attacks
- Social Engineering; and
- Password spraying

9.1.2 Windows 10 Credential Management Vulnerability

Windows Credential Manager is dependent on the user entering a password. The user password has these vulnerabilities:

- Shorter passwords are easier to crack
- Long or complex passwords are hard to remember, often resulting in help desk calls
- User-selected passwords often appear in rainbow tables; and
- Typical Windows user passwords must expire periodically.

The TOE described in this document solves the problems described above by supplementing the default Windows Credential Manager with another authentication method. With this supplement the user never enters a password, and each authentication request is unique. Use of the TOE allows passwords to be managed centrally as a long collection of random characters without user interaction. The TOE can be configured to change each user password in accordance with organisational policy, or more frequently.

9.1.3 Use of personal electronic devices for MFA in Secure Environments

Two factor or multi-factor authentication (MFA) relies on mechanisms and devices such as mobile phones or laptops that are incompatible with secure or austere operating environments. Examples may include secure facilities that do not allow the presence of personal electronic devices, recording devices or items that can store information. Mobile phones typically have a global position system (GPS), a microphone and can be infected with malware. Hardware tokens have known vulnerabilities and are expensive to maintain. Radio frequency identification (RFID) cards can be cloned. Contactless smart cards such as credit cards were vulnerable to simple man-in-the-middle attacks until a change in the payment card industry in 2013.

The TOE described in this document solves the problems described above by providing the bare minimum of functionality to implement MFA without the vulnerabilities of RFID cards and older contactless smart cards.

9.2 Introduction to the TOE

The VeroGuard HSM Digital ID for Open Networks solution (TOE) serves an MFA function by providing bespoke hardware that extends secure financial transaction technology. This is performed using a handheld terminal known as a VeroCard. This terminal can communicate with a server initially. Offline verification via the VeroCard personal identification number (PIN) keypad is available after initial use. Other features include Bluetooth operating in a secure mode for contactless communication in place of the familiar International Electrotechnical Commission (IEC) standard 14443 compliant contactless smart card.

Anywhere a contactless smart card or a chip-and-pin is used for authentication, the solution may also be used. Like chip-and-pin validation, the VeroCard user must enter a PIN to validate the use of the card. The VeroGuard HSM Digital ID solution relies on a generic Bluetooth device which uses the same USB port as many bespoke card readers. Any Bluetooth master device may be used.

The solution includes these features:

- The VeroCard is a bespoke PED that that has no user accessible memory, microphone, camera, or GPS so it poses no extra risk when operated in a secure environment.
- The VeroCard cannot be copied and is not vulnerable to a wide range of attacks due to the solution's features
- Management of VeroCards and users is by administrators familiar with Windows Active Directory
- An additional Windows Desktop Credential Provider to facilitate the use of a VeroCard for authentication via PIN entry instead of manual password entry; plus
- The solution can authenticate and administer a VeroCard via any compatible web browser including those on a Bluetooth enabled personal electronic device.

During manufacture the VeroCard is configured using a manufacturing Hardware Security Module (HSM) which creates and transfers secrets to the VeroCard. The manufacturing HSM creates, stores, and uses public key cryptography which is securely transferred to the production DocuSign HSM.

As part of the solution, the production DocuSign HSM performs decryption and comparison of the encrypted authentication requests sent by the VeroCard. To achieve this function the production DocuSign HSM stores the base derivation key in accordance with the Derived Unique Keys Per Transaction (DUKPT) key management scheme (American National Standard Institute [ANSI] X9.24-3-2017). The key exchange between the production DocuSign HSM and the VeroCard uses Elliptic-curve Diffie–Hellman (ECDH) key agreement protocol, identifying the VeroCard via information signed by the manufacturing HSM.

The TOE component VeroGuard SDKMod custom component performs VeroCard PIN Block validation.

See the document SPC_CC_004 VeroCard Key Loading Design & Implementation for detailed information on key loading and remote key injection.

9.3 Security Objectives of the TOE Components

This section describes the security objectives of each component in Table 3.

Security objectives include:

- Resource protection
- Authentication
- Authorization
- Integrity (Data integrity and System integrity)
- Nonrepudiation; and/or
- Confidentiality.

9.3.1 Manufacturing DocuSign HSM

The VMS manufacturing DocuSign HSM holds the root certificate and the manufacturers private key for the solution. This data is used by the manufacturing DocuSign HSM to emit a public key. The public key is used to electronically sign the VeroCard executable.

9.3.2 Keyloader

The VMS Keyloader executable is used to configure each VeroCard at the point of manufacture. The keyloader installs cryptographic keys including one key that allows the VeroCard to communicate securely during first use. The keyloader performs functions in accordance with American National Standards Institute (ANSI) standard X9.24 part 2 for distribution of symmetric keys. The security objective of this TOE component are authentication and confidentiality.

9.3.3 VeroCard

The VeroCard facilitates MFA by providing a user interface (PIN entry device or PED) where the user can enter a PIN. During PIN entry, the VeroCard transmits both its serial number and a terminal ID.

The VeroCard generates an ISO 9564-1 Format 4 PIN Block using the VeroCard serial number as the Primary Account Number (PAN).

The VeroCard sends the PIN Block in online mode during an authentication request.

In online mode the VeroCard can be revoked plus the PIN can be reset by the administrator.

The VeroCard stores a local hash of the PIN to facilitate authentication in offline mode. Offline mode authentication is enabled by the administrator of the application to allow for successful authentication when the production DocuSign HSM is not contactable.

VeroCard management and user management are separate functions and separate security objectives.

The VeroCard is initialised in accordance with ANSI X9.24 when communicating via VeroGuard.Card.Service.exe with the TOE Component VeroGuard.Terminal.Activate.Host.dll.

Once initialised, each VeroCard authentication request is validated when communicating via VeroGuard.Card.Service.exe with the TOE Component VeroGuard.Terminal.Host.dll.

The security objectives of the VeroCard are authentication, authorisation, and confidentiality.

9.3.4 Serenity Credential Provider

The Serenity Login Installer adds Serenity Credential Provider and disables other options on the Windows Login screen. The Serenity Login Installer itself has no security objectives. The Serenity Credential Provider that is installed uses the successful authentication with the VeroCard to retrieve credentials for the current user. The security objectives of the Serenity Credential Provider are authentication, authorisation, and confidentiality.

9.3.5 VeroBureau.API.exe

This component provides an endpoint for the service that maintains an Open LDAP database. The Open LDAP database maintains a relationship between an AD user and one or more VeroCards. The Open LDAP database references the Windows Active Directory security identifier (SID) of the current user.

The Open LDAP database stores the status of the card and some application permissions. Examples of permissions include login to windows, use Open ID Auth and view active directory.

The VeroBureau.API.exe component communicates with Windows Active Directory to determine if the AD user is inactive or has an expired password. This component also provides a second endpoint for Open ID functionality - provision of STS tokens as the Open ID server for each VeroCard.

The Open LDAP database is non-TOE.

The security objectives of this component are resource protection and authorization.

9.3.6 VeroGuard.Tms.exe

This component references VeroCards as terminals and facilitates VeroCard firmware upgrades, where configured by the administration. This component can enable or disable a card and is used to add a new card to the solution. If there is a difference between the VeroCard firmware and the details expected in the database used by this TOE component, one of the follow actions may occur:

- If the upgrade is marked as OPTIONAL, the firmware will be uploaded to the VeroCard. The user may then choose to use the new firmware by accessing the Upgrade option in the VeroCard menu; or
- If the upgrade is marked as FORCED, the upgrade will occur the next time the VeroCard connects to this TOE component.

See the document USG_CC_002 Terminal Management System (TMS) User Guide section 4.1.1 “Update version configuration” for information on firmware upgrades.

The security objectives of this component are authorization and system integrity.

9.3.7 VeroGuard.Card.Service.exe

This component receives the PIN Block requests including new PIN requests from the card then forwards the request to the TOE component VeroGuard.Hsm.Host.dll. If the PIN Block request is a PIN verification request, this request is forwarded to VeroGuard SDKMod custom component code. VeroGuard SDKMod custom component code is executed on the production DocuSign HSM. PIN retries are hard coded to 3 retries in this component. This component generates and returns any retry exceedance messages in support of non-repudiation. This component uses the SQL server database to record current retries, bad pin attempts lifetime count, and card activation state.

The security objectives of this component are non-repudiation, and authentication.

9.3.8 VeroGuard.Hsm.Host.dll and Production DocuSign HSM

VeroGuard.Hsm.Host.dll is a web service endpoint that is a wrapper for the production DocuSign HSM and facilitates its security objectives. APIs are used for encryption, decryption, and verification. This component only receives requests from VeroGuard.Terminal.Activate.Host.dll, VeroGuard.Terminal.Host.dll, and from VeroGuard.Card.Service.exe. The security objectives of the production DocuSign HSM are to encrypt, decrypt and verify requests from a VeroCard.

The production DocuSign HSM stores the manufacturer public key used at the time the VeroCards are manufactured.

The production DocuSign HSM decrypts the message containing the PIN Block but does not calculate PIN validity.

The security objectives of these components are authentication and confidentiality.

9.3.9 VeroGuard.Terminal.Host.dll

This component is a web service endpoint for card identity and card firmware management. Security objectives include:

- Accept requests from a VeroCard then send requests to VeroGuard.Card.Service.exe for PIN verification/set/change/replace (note the PIN is verified in the TOE component VeroGuard SDKMod custom component)
- Send requests to encrypt or decrypt to HSM Host as required to setup DUKPT
- Send requests to VeroBureau.API.exe to verify that a card is registered to a user; and
- Send requests to VeroBureau.API.exe to get resource (application) permissions

The security objectives of this component are resource protection, authentication, authorization, and nonrepudiation.

9.3.10 VeroGuard.Terminal.Activate.Host.dll

This component is used in the operational environment to activate the VeroCard for the first time. The initial communication of each VeroCard is with this TOE component in accordance with standard ANSI x9.24 Part 3. The initialisation is performed using AES 128-bit Future Keys generated using the DUKPT mechanism.

The security objectives of this component are authentication, authorization, and nonrepudiation.

9.3.11 VeroGuard SDKMod Custom Component

This TOE component is a custom Windows assembly that was installed to the production DocuSign HSM server. The production DocuSign HSM server then made an outbound call to the DocuSign manufacturer for final signing of the module, from the VeroGuard manufacturing premises. The VeroGuard SDKMod Custom Component (SDKMod) APIs are available to be called by VeroGuard.HSM.Host.DLL after the component is signed and the production DocuSign HSM is set to non-FIPS mode. The evaluated configuration includes SDKMod with the APIs available and the production DocuSign HSM set to non-FIPS mode. SDKMod performs validation of the ISO 9564-1 Format 4 (ISO-4) PIN Block plus IPEK generation and generation of the DUKPT Base Derivation Key ID (BDK ID) during Remote Key Injection (RKI).

Security objectives include: Authentication, Integrity and Confidentiality.

9.4 Physical Scope of the TOE

This section describes the physical layout of the TOE and Non-TOE components relative to the security problems from section 9.1.

Note: The term BoID refers to the TOE Component VeroBureau.API.exe plus the non-TOE component “slapd” which is an Ubuntu Linux service that maintains an Open LDAP database.

VeroGuard Services references all TOE components that are Windows executables except VeroBureau.API.exe and any custom components on the production DocuSign HSM.

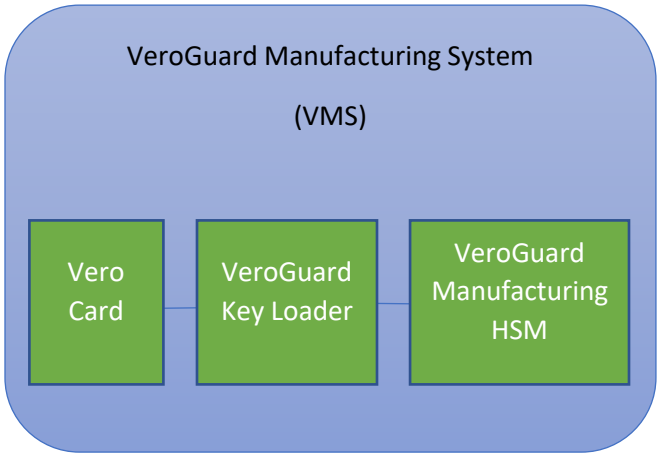

Figure 1: VeroGuard Manufacturing System

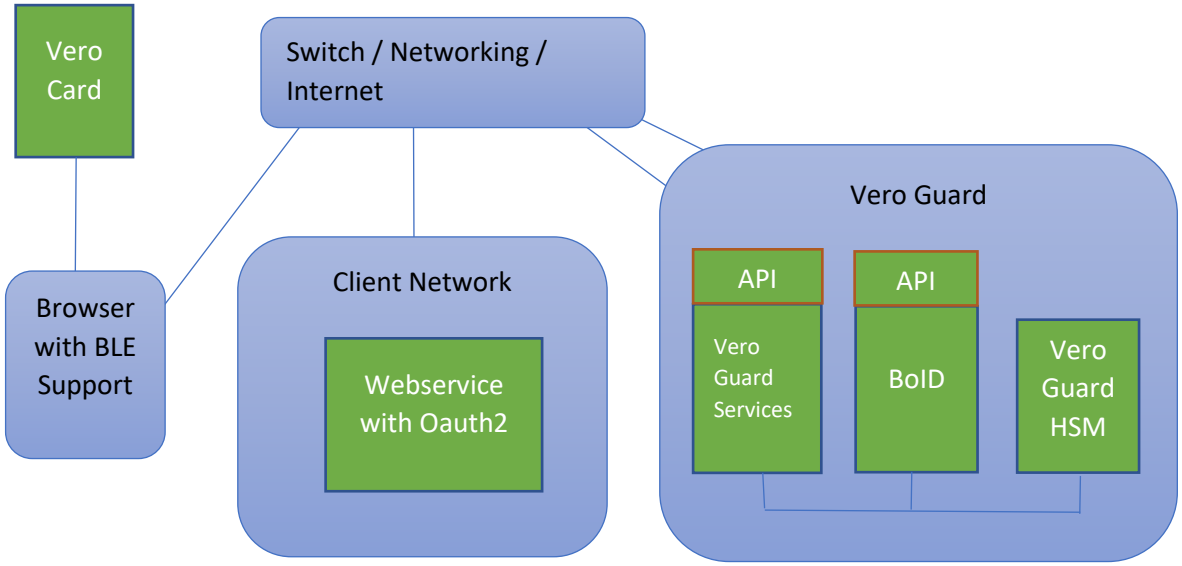

Figure 2: Physical Layout of TOE and Non-TOE items for Open ID Connect (OAuth2) use case

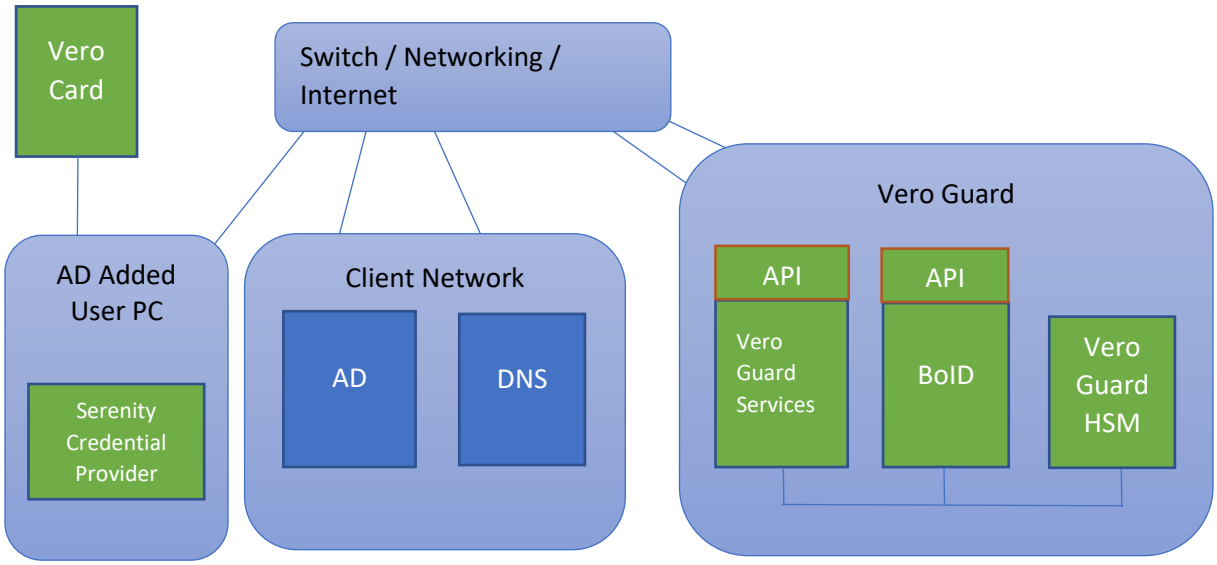

Figure 3: Physical Layout of TOE and Non-TOE components for Windows Active Directory

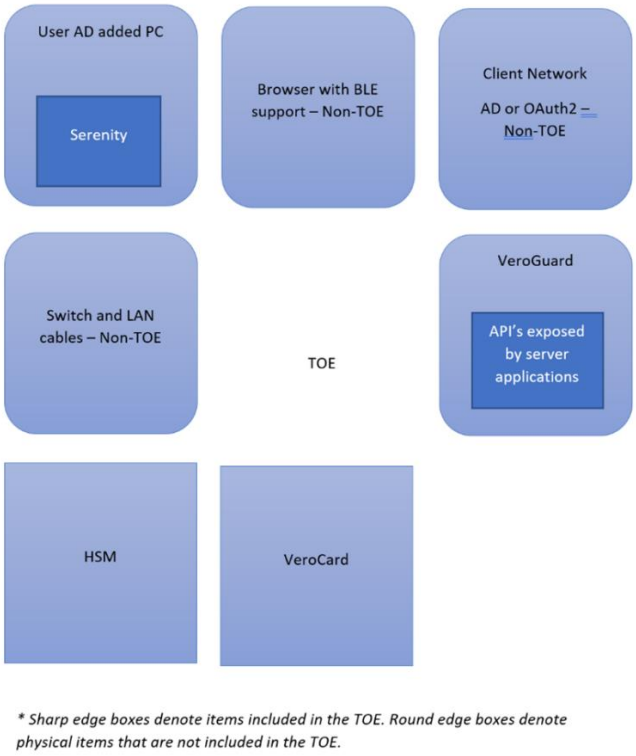

Figure 4: Logical Layout of TOE and Non-TOE items

10 Conformance Claims (ASE_CCL)

The ST and TOE claim conformance to

- Common Criteria v3.1 Revision 5 Part 1
- Common Criteria v3.1 Revision 5 Part 2; and
- Common Criteria v3.1 Revision 5 Part 3.

Common Criteria v3.1 Revision 5 Part 1 is fully identified in [CC Part 1], Common Criteria v3.1 Revision 5 Part 2 in [CC Part 2] and Common Criteria v3.1 Revision 5 Part 3 in [CC Part 3].

The ST is CC Part 2 Extended conformant.

The ST is CC Part 3 conformant.

The ST claims conformance to the following Protection Profiles: None.

The ST claims conformance to the assurance package Evaluation Assurance Level 2 augmented by ALC_FLR.1 (EAL2+).

10.1 Conformance Claims Rationale

The ST does not claim conformance to any Protection Profile. Therefore, the Conformance Claims Rationale is not applicable.

10.2 Claims Specific to VeroCard

The VeroCard is certified under Payment Card Industry (PCI) approval 4-4092. Point of Interaction (POI) requirements were verified under the certification PCI_PTS_POI_SRs_v5-1. View the table below for relevant claims:

Claim
The VeroCard implements measures which prevent measurable electromagnetic emissions
The VeroCard is constructed to be tamper evident
Mechanical tampering triggers zeriozation
The VeroCard protects data stored within it
Valid PIN codes are encrypted when entered
Attempts to replay a PIN transmission will not be successful

Table 4: VeroCard Claims and Verification

10.3 Claims Specific to DocuSign HSM

The TOE describes one manufacturing and one production DocuSign HSM. These items are the same part number. The manufacturing HSM is used as a root certificate authority. Prior to being shipped by the manufacturer, the production DocuSign HSM is loaded with a certificate containing the manufacturer public key. This certificate allows the VeroCard to verify authentic communication with the production DocuSign HSM on first use.

This section describes claims specific to the DocuSign HSM. As part of the TOE, the production DocuSign HSM is certified under NIST FIPS 140-2 compliance Certification 2860[1]. All claims below are verified by this certification.

Claim
Implements Symmetric Key Encryption and Decryption (the certificate notes AES, TDEA)
Implements Digital Signatures (DSA, RSA and ECDSA)
Implements Secure Hash Standard (SHS)
Implements SHA-3 Standard
Implements Message Authentication (the certificate notes Triple-DES, AES and HMAC)

Table 5: DocuSign HSM Claims

[1] https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/2860

11 Security Problem Definition (ASE_SPD)

Each element in this section is identified by a prefix and a short name, followed by a definition of the element. This section includes:

- Threats (T)
- Organizational Security Policies (OSP); and
- Assumptions (A).

11.1 Threats

The TOE is concerned with the following threats:

11.1.1 T.TAMPERED_PCB

An external party succeeds in tampering with components of the VeroCard Printed Circuit Board (PCB) to inject malicious executables into the manufactured item.

11.1.2 T.UNKNOWN_STATE

A legitimate user of the VeroCard manages the VeroCard in a manner which causes transfer of the VeroCard software to an unknown, insecure state. This state may allow unauthorised access to associated services.

11.1.3 T.EMSEC

An unauthorised party reads and records electromagnetic emanations from the VeroCard during normal operation. Secrets relevant to the VeroCard or the user of the TOE can be determined from these recordings and used for unauthorised access.

11.1.4 T.PHYSICAL_TAMPERING_V

An unauthorised party physically accesses the secure memory of the VeroCard. The data is read and used to clone or emulate the VeroCard without detection.

11.1.5 T.PHYSICAL_TAMPERING_H

The DocuSign HSM can be copied or configured to allow inauthentic cards to be validated.

11.1.6 T.LOGICAL_TAMPERING

An unauthorised party modifies VeroCard executables to allow loading and/or storing of cryptographic keys in memory areas that are not secure.

11.1.7 T.FAKE_FW

An unauthorised party replaces a legitimate executable uploaded to the VeroCard to force unauthentic behaviour. FW refers specifically to the firmware installed on the VeroCard during manufacture or update.

11.1.8 T.EAVES_P

An unauthorised party eavesdrops the PIN Block sent from the VeroCard. The unencrypted PIN is determined from the eavesdropped data.

11.1.9 T.EAVES_N

A malicious user eavesdrops on network traffic communication between the TOE components VeroGuard.HSM.Host.dll and the production DocuSign HSM to gain unauthorized access to TOE data.

11.1.10 T.INCORRECT_TIME

A malicious administrator changes the server time configuration after the VeroCard enters the lifecycle state “Active”. The card sends a freshness (time) value that is very different to the server time or the server sends a different time to the current PED time.

11.1.11 T.WEAKIA

A malicious user could be illicitly authenticated through brute-force guessing of credentials. An external party attempts to guess the PIN of the VeroCard multiple times.

11.1.12 T.WEAKPOL

Policies that facilitate robust access control are absent or a careless administrator fails to enforce these policies. This threat may cause the TOE to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

11.1.13 T.UNAUTHENTIC_CREDENTIALS

A malicious user modifies their credentials gain access to resources.

11.1.14 T.UNAUTHORISED_USER

An unauthorised user gains access to resources.

11.1.15 T.CREDENTIAL_DISCOVERED

A malicious user gains access to authentic credentials for later impersonation.

11.1.16 T.UNEXPECTED_BEHAVIOUR

The VeroCard or other TOE component exhibits a flaw or unexpected behaviour typically addressed by upgrading to a new executable.

11.2 Organizational Security Policies

The TOE is governed by Organizational Security Policies in the following sections:

- OSP.PROTECT
- OSP.SECURE_MANUFACTURE
- OSP.PIN_QUALITY
- OSP.ISSUANCE
- OSP.HANDLING
- OSP.PASSWORD_QUALITY; and
- OSP.PASSWORD_VALIDITY_PERIOD

11.2.1 OSP.PROTECT

The following assumptions regarding protection are made:

- Secure erasure during manufacture
- Removal of Key Loader executable; and
- Mandatory Zeroization and PIN Policy Enforcement.

11.2.2 OSP.SECURE_MANUFACTURE

With exception to stated security objectives, the physical premises being used for the manufacture of the TOE is sufficiently secured against malicious attackers.

11.2.3 OSP.PIN_QUALITY

Each backend application which uses the VeroCard for authenticating users has determined and enforced a minimum PIN code length in accordance with the security requirements of the application.

The application also has determined the minimum quality requirements for the PIN codes (e.g. a PIN code 123456 should not be used) which are communicated to the user and enforced by the application.

11.2.4 OSP.ISSUANCE

The organisation using the TOE has defined and enforced a policy that governs the identification and authentication requirements of the user prior to granting access to the application and issuing them a VeroCard. The policy must be aligned with the applicable laws that govern identification and authentication as well as protection of the physical documents used in identification and authentication once the identity of the user is determined.

11.2.5 OSP.HANDLING

The organisation issuing the VeroCard to the users has defined and communicated to the users the requirements for secure handling of the VeroCard. Instances of the VeroCard are only issued to users committed to conforming with the VeroCard handling requirements. These requirements govern issues such as how to store the VeroCard when not used to minimise the opportunities for physical attack, how to inspect the VeroCard for signs of physical tampering, and how to ensure that the environment in which the VeroCard is used is such that PIN entry is not observed by third parties.

11.2.6 OSP.PASSWORD_QUALITY

The organisation controlling user password quality has a policy that is aligned with the password quality enforced by the TOE component VeroGuard.TMS.exe. The password created and updated by the TOE component has a length of 19 characters of mixed case with numbers and non-alphanumeric values. The password quality policy cannot require a more complex password than this.

11.2.7 OSP.PASSWORD_VALIDITY_PERIOD

The organisation controlling user password validity period has a policy that is aligned with the password lifetime enforced by the TOE component VeroGuard.TMS.exe. The value is configurable in the TOE and the TOE component shall update the user password more often than the policy requires.

11.3 Assumptions

Assumptions regarding the TOE appear below:

- A.LOCATE
- A.MANAGE
- A.NOEVIL; and
- A.PLATFORM

11.3.1 A.LOCATE

The manufacturing HSM and the production DocuSign HSM and application servers will be located within controlled access facilities, which will prevent unauthorized physical access.

11.3.2 A.MANAGE

Individuals managing the TOE are competent. Users have (and understand) comprehensive user manuals that describe:

- Organisational security policies
- Administration, Configuration, and maintenance
- The number of invalid PIN entry attempts before the VeroCard erases its PIN hash; and
- Operation instructions.

11.3.3 A.NOEVIL

The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided. This assumption is supported by the operational environment objectives OE.ISSUANCE, OE.MANAGE, OE.PROTECT and OE.USERS.

11.3.4 A.PLATFORM

The platform is described by:

- the physical locations where the VeroCard is manufactured and used
- the information technology infrastructures such as switches, racks, and rooms
- other network hardware used to support the operation of the production DocuSign HSM
- operating systems and servers that host TOE components such as VeroBureau.API.exe; and
- the environment in which the VeroCard is issued.

The platform that the TOE is deployed in is sufficient to prevent unauthorized access.

The operating environment objectives OE.PCB_AUTH and OE.MANAGE are supported by this assumption.

12 Security Objectives (ASE_OBJ)

This section describes:

- Security objectives for the operational environment; and
- Security objectives for the TOE.

12.1 Security Objectives for the Operational Environment (ASE_OBJ.1)

The following security objectives are applicable for the operational environment (OE):

- OE.PCB_AUTH
- OE.ISSUANCE
- OE.HANDLING
- OE.MANAGE
- OE.PHYSICAL
- OE.PROTECT; and
- OE.USERS

12.1.1 OE.PCB_AUTH

The VMS shall include a secure manufacturing process that erases all executables and data on the components mounted on the VeroCard PCB Board. The VeroCard shall then be loaded with known authentic versions. This security objective of the operational environment counters the threats T.TAMPERED_PCB, T.FAKE_FW and T.UNEXPECTED_BEHAVIOUR.

12.1.2 OE.ISSUANCE

The issuance protocol and process for the VeroCard by the TOE Operator is defined in accordance with the national and other applicable laws, good privacy and security practices, and the security requirements of the relevant application. The protocol and process are strictly adhered to in the issuance of the instances of the VeroCard and sufficient records are generated, stored, and periodically audited by the relevant authorities.

This operational environment objective counters the threats T.UNAUTHORISED_USER and T.PHYSICAL_TAMPERING_V. The objective enforces OSP.ISSUANCE and upholds assumption A.MANAGE.

12.1.3 OE.HANDLING

The user issued with a VeroCard handles it with due care in accordance with the guidance and policies of the issuing organisation and periodically examines it for any signs of physical tampering.

This operational environment objective counters the threats T.PHYSICAL_TAMPERING_V and T.UNEXPECTED_BEHAVIOUR. The objective enforces OSP.HANDLING and upholds assumption A.PLATFORM.

12.1.4 OE.MANAGE

Those responsible for TOE deployment will provide competent administrators and users with appropriate training in accordance with guidance and will manage appropriate administration of the TOE. This operational environment objective counters the threats T.UNAUTHORISED_USER and T.PHYSICAL_TAMPERING_V. The objective enforces OSP.ISSUANCE and upholds assumption A.MANAGE.

12.1.5 OE.PHYSICAL

Those responsible for the VeroCard must ensure that the VeroCard is protected from any physical attack and that PIN entry operation is not viewed by other parties. Those responsible for the manufacture of the VeroCard and the configuration of each DocuSign HSM must ensure the hardware and executables are always secure.

This operational environment objective counters the threats T.PHYSICAL_TAMPERING_H and T.PHYSICAL_TAMPERING_V. The objective enforces OSP.ISSUANCE and upholds assumption A.MANAGE.

12.1.6 OE.PROTECT

Those responsible for the TOE must ensure that TOE components are protected from interference, tampering and physical attack. All hardware and executables in the TOE are protected.

This operational environment objective counters the threats T.PHYSICAL_TAMPERING_H and T.PHYSICAL_TAMPERING_V. The objective enforces OSP.PROTECT.

12.1.7 OE.USERS

Users issued a VeroCard interacts with the TOE and its applicable IT-Systems in the way it is intended.

This operational environment objective counters the threats T.PHYSICAL_TAMPERING_H, T.PHYSICAL_TAMPERING_V, T.EAVES_P, T.WEAKIA, T.WEAKPOL AND T.UNAUTHORISED_USER. The objective enforces OSP.HANDLING and OSP.PROTECT.

12.2 Security Objectives for the TOE (ASE_OBJ.2)

This section describes the following security objectives (O) for the TOE:

- O.PCB_AUTH
- O.MANAGEMENT

- O.EMSEC
- O.PHYSICAL_INTEGRITY
- O.DATA_INTEGRITY; and
- O.PIN_PROTECTION

12.2.1 O.PCB_AUTH

This security objective is related to OE.PCB_AUTH. The VeroCard manufacturing process shall erase all executables and data on the components mounted on the VeroCard PCB Board. The VeroCard shall then be loaded with known authentic versions. This objective mitigates the threats T.TAMPERED_PCB, T.FAKE_FW and T.UNEXPECTED_BEHAVIOUR.

The TOE manufacturer implemented secure executable and data erasure of the PCB component (FDP_RIP.1/PCB_SW) at the start of manufacture (O.PCB_AUTH).

12.2.2 O.MANAGEMENT

The VeroCard includes one user interface. Use of the interface will result in a secure state. Each DocuSign HSM has one secure physical interface and one secure client agent application. The Serenity Credential Provider has one interface. Use of this interface will result in secure states. These interfaces control when and how the user is authenticated.

This objective mitigates the threats T.UNKNOWN_STATE, T.UNEXPECTED_BEHAVIOUR and T.UNATHENTIC_CREDENTIALS.

The TOE manufacturer implemented the following management features to provide secure management for the TOE (O.MANAGEMENT):

- Subset access control when importing cryptographic keys (FDP_ACC.1.1)
- Security attribute-based access control using a keyloaded state (FDP_ACF.1.1 and FDP_ACF.1.2)
- Role-based access control for administration function (FDP_ACF.1.3)
- State-based access control to deny access in certain situations (FDP_ACF.1.4)
- Deallocation of the Keyloader software from the VeroCard during the manufacturing process (FDP_RIP.1/Keyloader)
- Establishment of a Bluetooth connection and authentication of the VeroCard on behalf of the user before the user is authenticated (FIA_UAU.1.1)
- Display of each entered PIN digit as an asterisk symbol to the user while the authentication is in progress (FIA_UAU.7.1)
- Some functions on the VeroCard to be accessed before the user is identified (FIA_UID.1)
- No user can change the cryptographic keys or lifecycle state (FMT_MSA.1)
- Deny access that would allow alternative keys to be loaded to a VeroCard (FMT_MSA.3)
- Management functions available during the manufacturing and operation of the VeroCard (FMT_SMF.1.1)
- Implement specified roles required for RBAC (FMT_SMR.1)

- Implement encrypted communication between the keyloader software and the manufacturing DocuSign HSM and between the TOE component VeroGuard.HSM.Host.DLL and the production DocuSign HSM (FPT_ITC.1)
- Provide reliable time stamps (FPT_STM.1); and
- Implement regularly executed self-tests in the TOE components manufacturing DocuSign HSM, production DocuSign HSM and VeroCard (FPT_TST.1)

12.2.3 O.EMSEC

The VeroCard prevents electromagnetic emanations useful for deduction of cryptographic keys or other secrets from being detected outside the VeroCard. The manufacturing and production DocuSign HSMs prevent electromagnetic emanations useful for deduction of cryptographic keys or other secrets from being detected outside either DocuSign HSM. This objective mitigates the threat T.EMSEC.

The TOE manufacturer implemented the following features to prevent intelligible emissions or useful interface emanations from the TOE (O.EMSEC):

- Shielding of the manufacturing and production DocuSign HSMs and shielding of the VeroCard achieves “no intelligible emissions” (FPT_EMS.1.1) and “no useful interface emanations” (FPT_EMS.1.2) that enable access to TSF data or user data
- The manufacturing and production DocuSign HSMs plus the VeroCard provide passive detection of physical tampering intended to bypass shielding (FPT_PHP.1); and
- The manufacturing and production DocuSign HSMs plus the VeroCard provide resistance to physical tampering intended to bypass shielding (FPT_PHP.3).

12.2.4 O.PHYSICAL_INTEGRITY

The VeroCard case is tamper evident. Tampering attempts on the VeroCard trigger zeroization. The DocuSign HSM is tamper evident. Tampering attempts on a DocuSign HSM trigger zeroization. This objective mitigates the threats T.TAMPERED_PCB, T.PHYSICAL_TAMPERING_H and T.PHYSICAL_TAMPERING_V.

The TOE manufacturer implemented the following features to ensure integrity, detect the loss of TOE component physical integrity, and to respond securely (O.PHYSICAL_INTEGRITY):

- The manufacturing and production DocuSign HSMs plus the VeroCard provide detection of physical tampering (FPT_PHP.1); and
- The manufacturing and production DocuSign HSMs plus the VeroCard provide resistance to physical tampering (FPT_PHP.3).

12.2.5 O.DATA_INTEGRITY

Use of the Serenity Credential Provider for authentication and authorisation shall be attributable.

Use of the VeroCard for authentication and authorisation shall be attributable. Use of the TOE for authentication and authorisation shall be legible.

Attributable data means organizations should know how data is created or obtained, and by whom. Legible data means organizations should be able to read and understand the data and the logs are permanent.

Use of the TOE for authentication and authorisation shall be contemporaneous: This part of data integrity means organizations should know how data appeared in its initial state and what happened to it throughout the different stages of its lifecycle.

Secrets used for authentication and authorisation shall be original: This aspect of data integrity implies an understanding of the TOE and attached systems and the ability to keep source data such as in each HSM in the original state.

Log information shall be stored in a way that allows prompt forensic investigation of unexpected behaviour. Logging of the use of Serenity Credential Provider is performed by the non-TOE component Windows Operating System.

Use of the TOE for authentication and authorisation shall be accurate: Accurate data includes accurate time. Accurate data is errorless and conforms to the protocols of the applications for which it is used.

This objective mitigates the threats T.LOGICAL_TAMPERING, T.FAKE_FW, T.EAVES_N, T.INCORRECT_TIME, T. WEAKIA, T.WEAKPOL, T.UNAUTHENTIC_CREDENTIALS, T.CREDENTIAL_DISCOVERED and T.UNEXPECTED_BEHAVIOUR. This objective enforces the organisational security policies OSP.PROTECT, OSP.SECURE_MANUFACTURE, OSP.PASSWORD_QUALITY and OSP.PASSWORD_VALIDITY_PERIOD.

The TOE manufacturer implemented the following features to ensure integrity, detect the loss of TOE data integrity, and to respond securely (O.DATA_INTEGRITY):

- Implement cryptographic support in the manufacturing and production DocuSign HSMs plus the VeroCard (FCS_CKM.1)
- Perform cryptographic operation in manufacturing and production DocuSign HSMs plus the VeroCard (FCS_COP.1.1/ECC256)
- Perform AES encryption of data-at-rest (keys) within the VeroCard (FCS_COP.1.1/AES)
- Perform TLS1.2 encryption using SHA256 between the keyloader and the manufacturing DocuSign HSM, and between the TOE component VeroGuard.HSM.Host.DLL and the production DocuSign HSM (FCS_COP.1.1/SHA-256). Note that stored hashes of the user PIN with SHA-256 is a different objective
- Control when keys can and cannot be imported to the VeroCard (FDP_ACC.1)
- Ensure that once keys are imported to the VeroCard, the lifecycle state of the VeroCard is changed to “Keyloaded” and key import cannot be successfully re-attempted (FDP_ACF.1)
- Enforce the use of the security attributes (data) provided by the VMS to the keyloader, only (FDP_ITC.2)

- Ensure the VMS removes the keyloader executable from the VeroCard near the end of manufacturing and verifies the executable is absent (FDP_RIP.1/Keyloader)
- Execute authentication failure handling including management of the stored hash of the PIN on the VeroCard (data) and creation of logs (data) that capture the authentication failure events (FIA_AFL.1)
- TOE components production DocuSign HSMs and the VeroCard implement random number generators. This generated data is required to pad selected messages to resist replay (FIA_SOS.2)
- Enforce default values (data) provided by the VMS to the keyloader, only (FMT_MSA.3)
- Read and write data on the VeroCard during manufacturing and operation (FMT_SMF.1)
- Implement RBAC for reading and writing of data throughout the TOE (FMT_SMR.1)
- Ensure the to be TOE secure during attempted physical or logical tampering (FPT_FLS.1)
- Ensure data transmitted between the keyloader and the manufacturing DocuSign HSM and between the TOE component VeroGuard.HSM.Host.DLL and the production DocuSign HSM are kept confidential (FPT_ITC.1)
- Ensure the cryptographic keys (data) including the manufacturer's public key stored on the VeroCard are consistently interpreted by the production DocuSign HSM (FPT_TDC.1); and
- Implement secure communication between the keyloader and the manufacturing DocuSign HSM and between the TOE component VeroGuard.HSM.Host.DLL and the production DocuSign HSM (FTP_ITC.1)

12.2.6 O.PIN_PROTECTION

User PIN codes are protected from guessing, disclosure or modification when communicated or stored. This objective mitigates the threats T.EAVES_P, T.LOGICAL_TAMPERING and T.UNAUTHORISED_USER. This objective supports the organisational security policy OSP.PIN_QUALITY.

The TOE manufacturer implemented the following features to ensure PIN code protection (O.PIN_PROTECTION):

- Implement and use DUKPT for key distribution to the VeroCard. These keys are used to encrypt the transmission of user PIN related data (FCS_CKM.2.1/DUKPT)
- Implement and use ECDH for key distribution to the VeroCard. ECDH is used for remote key injection during activation of the VeroCard (FCS_CKM.2/ECDH)
- The VeroCard shall zeroize all data including the stored hash of the user PIN during its tamper response, also erase the user PIN stored on the VeroCard after three (3) unsuccessful PIN entry attempts (FCS_CKM.4)
- Implement encryption of VeroCard key initialisation messages using ECC256 to allow for subsequent user PIN attempt transmission (FCS_COP.1.1/ECC256)
- Implement stored PIN digest computation on the VeroCard (FCS_COP.1.1/SHA-256); and
- A new user PIN entered on the VeroCard replaces the previous user PIN entered (FDP_RIP.1/PIN)

12.3 Security Objectives Rationale

The security objectives rationale:

- Traces each security objective for the TOE (O) back to threats (T) countered by that security objective
- Traces each security objective for the TOE (O) to organisational security policies (OSPs)
- Traces each security objective for the Operational Environment (OE) back to threats (T) countered by that security objective; and
- Traces each security objective for the Operational Environment (OE) to organisational security policies (OSPs) and assumptions (A).

An image of the mapping required appears below from Common Criteria Part 1[2]:

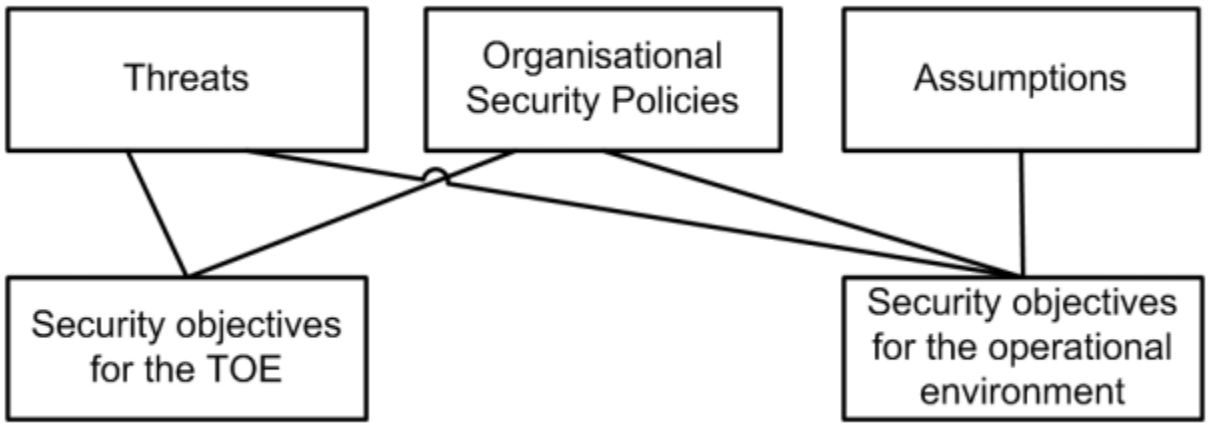

Figure 5: Mapping of Security Objectives to Threats, Policies and Assumptions

[2] https://commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf page 75

This table traces each security objective for the TOE (O) back to threats (T) countered by that security objective and in the lower rows, traces each security objective for the TOE back to Organisational Security Policies (OSP) enforced or upheld by that security objective.

	T.TAMPERED_PCB	T.UNKNOWN_STATE	T.EMSEC	T.PHYSICAL_TAMPERING_V	T.PHYSICAL_TAMPERING_H	T.LOGICAL_TAMPERING	T.FAKE_FW	T.EAVES_P	T.EAVES_N	T.INCORRECT_TIME	T.WEAKIA	T.WEAKPOL	T.UNAUTHENTIC_CREDENTIALS	T.UNAUTHORISED_USER	T.CREDENTIAL_DISCOVERED	T.UNEXPECTED_BEHAVIOUR	OSP.PROTECT	OSP.SECURE_MANUFACTURE	OSP.PIN_QUALITY	OSP.ISSUANCE	OSP.HANDLING	OSP.PASSWORD_QUALITY	OSP.PASSWORD_VALIDITY_PERIOD
O.PCB_AUTH	X						X									X							
O.MANAGEMENT		X											X			X							
O.EMSEC			X																				
O.PHYSICAL_INTEGRITY	X			X	X															X	X		
O.DATA_INTEGRITY						X	X		X	X	X	X	X		X	X	X	X				X	X
O.PIN_PROTECTION						X		X						X					X				

Table 6: Tracing of the Security Objectives (O) to Threats (T) and Organisational Security Policies (OSP)

Assumptions and Organisational Security Policies Security appear in the subsequent table for formatting reasons. Objectives for the Operational Environment (OE) are traced to threats (T) using the table below:

	T.TAMPERED_PCB	T.UNKNOWN_STATE	T.EMSEC	T.PHYSICAL_TAMPERING_V	T.PHYSICAL_TAMPERING_H	T.LOGICAL_TAMPERING	T.FAKE_FW	T.EAVES_P	T.EAVES_N	T.INCORRECT_TIME	T.WEAKIA	T.WEAKPOL	T.UNAUTHENTIC_CREDENTIALS	T.UNAUTHORISED_USER	T.CREDENTIAL_DISCOVERED	T.UNEXPECTED_BEHAVIOUR
OE.PCB_AUTH	X						X									X
OE.ISSUANCE				X									X	X		
OE.HANDLING							X			X					X	X
OE.MANAGE									X	X	X	X		X		
OE.PHYSICAL							X	X								
OE.PROTECT				X	X	X				X	X			X	X	
OE.USERS								X		X						

Table 7: Tracing Operating Environment security objectives (OE) to Threats (T)

Security objectives for the Operational Environment (OE) are traced to Organisational Security Policies (OSP) and assumptions (A) using the table below:

	OSP.PIN_QUALITY	OSP.ISSUANCE	OSP.HANDLING	OSP.PASSWORD_QUALITY	OSP.PASSWORD_VALIDITY_PERIOD	OSP.PROTECT	OSP.SECURE_MANUFACTURE	A.LOCATE	A.MANAGE	A.NOEVIL	A.PLATFORM
OE.PCB_AUTH						X	X				X
OE.ISSUANCE		X							X	X	
OE.HANDLING			X						X		
OE.MANAGE			X	X	X			X	X	X	X
OE.PHYSICAL			X				X		X		
OE.PROTECT							X		X	X	
OE.USERS	X								X	X	

Table 8: Operating Environment security objectives (OE) mapped to Organisational Security Policies (OSP) and Assumptions (A)

12.3.1 Threats Tracing to Security Objectives and Security Objectives of the TOE environment rationale

12.3.1.1 T.TAMPERED_PCB

OE.PCB_AUTH This objective requires that the VMS erases all executables and data mounted on the VeroCard PCB then loads an authentic version ensuring authentic installation on each PCB.

O.PHYSICAL_INTEGRITY This objective requires that the VeroCard case is tamper evident. Tampering attempts on the VeroCard trigger zeroization. The DocuSign HSM is tamper evident. Tampering attempts on the DocuSign HSM trigger zeroization.

O.PCB_AUTH The VeroCard manufacturing process shall erase all executables and data on the components mounted on the VeroCard PCB Board. The VeroCard shall then be loaded with known authentic versions.

12.3.1.2 T.UNKNOWN_STATE

O.MANAGEMENT The VeroCard includes one user interface. Use of the interface will result in a secure state. Each DocuSign HSM has one secure physical interface and one secure client agent application. The Serenity Credential Provider has one interface. Use of this interface will result in secure states. These interfaces control when and how the user is authenticated.

12.3.1.3 T.EMSEC

O.EMSEC The VeroCard prevents electromagnetic emanations useful for deduction of cryptographic keys or other secrets from being detected outside the VeroCard.

12.3.1.4 T.PHYSICAL_TAMPERING_V

OE.ISSUANCE The protocol and process are strictly adhered to in the issuance of the instances of the VeroCard and sufficient records are generated, stored, and periodically audited by the relevant authorities.

OE.PROTECT Those responsible for the TOE must ensure that TOE components are protected from interference, tampering and physical attack. All hardware and executables in the TOE are protected.

O.PHYSICAL_INTEGRITY The VeroCard case is tamper evident. Tampering attempts on the VeroCard trigger zeroization.

12.3.1.5 T.PHYSICAL_TAMPERING_H

OE.PROTECT Those responsible for the TOE must ensure that TOE components are protected from interference, tampering and physical attack. All hardware and executables in the TOE are protected.

O.PHYSICAL_INTEGRITY The VeroCard case is tamper evident. Tampering attempts on the VeroCard trigger zeroization. The DocuSign HSM is tamper evident. Tampering attempts on the DocuSign HSM trigger zeroization.

12.3.1.6 T.LOGICAL_TAMPERING

OE.PROTECT mitigates this threat when those responsible for the TOE must ensure that TOE components are protected from interference, tampering and physical attack. All hardware and executables in the TOE are protected.

O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be accurate: Accurate data is errorless and conforms to the protocols of the applications for which it is used. Use of the TOE for authentication and authorisation shall be contemporaneous: This part of data integrity means organizations should know how data appeared in its initial state and what happened to it throughout the different stages of its lifecycle.

O.PIN_PROTECTION User PIN codes are protected from disclosure or modification when communicated or stored.

12.3.1.7 T.FAKE_FW

OE.PCB_AUTH The VMS shall include a secure manufacturing process that erases all executables and data on the components mounted on the VeroCard PCB Board including any that were installed prior to the start of component picking.

OE.HANDLING The user issued with a VeroCard handles it with due care in accordance with the guidance and policies to detect tampering that may lead or have led to a firmware change.

OE.PHYSICAL Those responsible for the manufacture of the VeroCard and the configuration of each DocuSign HSM must ensure the hardware and executables are always secure.

O.PCB_AUTH The VeroCard manufacturing process shall erase all executables and data on the components mounted on the VeroCard PCB Board. The VeroCard shall then be loaded with known authentic versions.

O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be contemporaneous: This part of data integrity means organizations should know how data appeared in its initial state and what happened to it throughout the different stages of its lifecycle.

12.3.1.8 T.EAVES_P

OE.PHYSICAL Those responsible for the VeroCard must ensure that the VeroCard is protected from any physical attack and that PIN entry operation is not viewed by other parties.

OE.USERS Users issued a VeroCard interacts with the TOE and its applicable IT-Systems in the way it is intended. Meeting this objective reduces opportunities to change the firmware.

O.PIN_PROTECTION User PIN codes are protected from guessing, disclosure or modification when communicated or stored.

12.3.1.9 T.EAVES_N

OE.MANAGE Those responsible for TOE deployment will provide competent administrators and users with appropriate training in accordance with guidance and will manage administration appropriate of the TOE.

O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be contemporaneous: This part of data integrity means organizations should know how data appeared in its initial state and what happened to it throughout the different stages of its lifecycle.

12.3.1.10 T.INCORRECT_TIME

O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be accurate: Accurate data is errorless and conforms to the protocols of the applications for which it is used.

OE.HANDLING The user issued with a VeroCard handles it with due care in accordance with the guidance and policies of the issuing organisation and periodically examines it for any signs of physical tampering.

OE.MANAGE Those responsible for TOE deployment will provide competent administrators and users with appropriate training in accordance with guidance and will manage administration appropriate of the TOE.

OE.PROTECT Those responsible for the TOE must ensure that TOE components are protected from interference, tampering and physical attack.

OE.USERS Users issued a VeroCard interacts with the TOE and its applicable IT-Systems in the way it is intended.

12.3.1.11 T.WEAKIA

OE.MANAGE Those responsible for TOE deployment will provide competent administrators and users with appropriate training in accordance with guidance and will manage administration appropriate of the TOE.

OE.PROTECT Meeting this objective ensures all hardware and executables in the TOE are protected, reducing the opportunity for a malicious user to craft and execute a brute force attack undetected.

O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be accurate: Accurate data is errorless and conforms to the protocols of the applications for which it is used. Meeting this objective ensures malicious activity is detected.

12.3.1.12 T.WEAKPOL

O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be contemporaneous: This part of data integrity means organizations should know how data appeared in its initial state and what happened to it throughout the different stages of its lifecycle.

OE.MANAGE Those responsible for TOE deployment will provide competent administrators and users with appropriate training in accordance with guidance and will manage administration appropriate of the TOE. Meeting this objective ensures policies are appropriately followed.

12.3.1.13 T.UNATHENTIC_CREDENTIALS

OE.ISSUANCE The protocol and process are strictly adhered to in the issuance of the instances of the VeroCard and sufficient records are generated, stored, and periodically audited by the relevant authorities. Meeting this objective ensures malicious activity is detected.

O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be contemporaneous: This part of data integrity means organizations should know how data appeared in its initial state and what happened to it throughout the different stages of its lifecycle. Meeting this objective ensures malicious activity does not result in loss of data integrity.

O.MANAGEMENT Use of the interface will result in a secure state. Meeting this objective ensures malicious activity does not result in an insecure state.

12.3.1.14 T.UNAUTHORISED_USER

OE.ISSUANCE The issuance protocol and process for the VeroCard by the TOE Operator is defined in accordance with the national and other applicable laws, good privacy and security practices, and the security requirements of the relevant application. The protocol and process are strictly adhered to in the issuance of the instances of the VeroCard and sufficient records are generated, stored, and periodically audited by the relevant authorities.

OE.MANAGE Those responsible for TOE deployment will provide competent administrators and users with appropriate training in accordance with guidance and will manage appropriate administration of the TOE. Meeting this objective ensures that unauthorised users will be denied an opportunity to attempt malicious action.

OE.USERS Users issued a VeroCard interacts with the TOE and its applicable IT-Systems in the way it is intended. Meeting this objective ensures that unauthorised users will be denied an opportunity to attempt malicious action.

O.PIN_PROTECTION User PIN codes are protected from guessing, disclosure or modification when communicated or stored. Meeting this objective ensures that unauthorised users will not successfully execute typical sociological, replay other more technical attacks.

12.3.1.15 T.CREDENTIAL_DISCOVERED

OE.HANDLING mitigates this threat when the VeroCard user handles it with due care in accordance with the guidance and policies of the issuing organisation

OE.PROTECT mitigates this threat when all hardware and executables in the TOE are protected.

O.DATA_INTEGRITY Use of the Serenity Credential Provider for authentication and authorisation shall be attributable. Use of the VeroCard for authentication and authorisation shall be attributable. Attributable data means organizations should know how data is created or obtained, and by whom. Legible data means organizations should be able to read and understand the data and the logs are permanent.

12.3.1.16 T.UNEXPECTED_BEHAVIOUR

OE.PCB_AUTH The VeroGuard Manufacturing System (VMS) shall include a secure manufacturing process that erases all executables and data on the components mounted on the VeroCard PCB Board.

OE.HANDLING The user issued with a VeroCard handles it with due care in accordance with the guidance and policies of the issuing organisation and periodically examines it for any signs of physical tampering.

O.PCB_AUTH The VeroCard manufacturing process shall erase all executables and data on the components mounted on the VeroCard PCB Board.

O.MANAGEMENT Use of interfaces interface will result in secure states. These interfaces control when and how the user is authenticated.

O.DATA_INTEGRITY Use of the Serenity Credential Provider for authentication and authorisation shall be attributable. Use of the VeroCard for authentication and authorisation shall be attributable. Use of the TOE for authentication and authorisation shall be legible.

12.3.2 Organizational Security Policy Tracing to Security Objectives and Security Objectives of the TOE environment rationale

12.3.2.1 OSP.PROTECT

The policies regarding protection are:

- Secure erasure of new PCBs during manufacture
- Removal of Key Loader executable; and
- Mandatory Zeroization and PIN Policy Enforcement.

OE.PCB_AUTH The VMS shall include a secure manufacturing process.
O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be contemporaneous: This part of data integrity means organizations should know how data appeared in its initial state and what happened to it throughout the different stages of its lifecycle.

12.3.2.2 OSP.SECURE_MANUFACTURE

OE.PCB_AUTH pertains to a core part of VeroGuard manufacture.

OE.PHYSICAL and OE.PROTECT assumes that not only the intended users but the vendor producing the VeroCard is handling and appropriately protecting TOE components.

O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be contemporaneous: This part of data integrity means organizations should know how data appeared in its initial state and what happened to it throughout the different stages of its lifecycle.

12.3.2.3 OSP.PIN_QUALITY

OE.MANAGE Those responsible for TOE deployment will provide competent administrators and users with appropriate training in accordance with guidance and will manage appropriate administration of the TOE.

O.PIN_PROTECTION User PIN codes are protected from guessing, disclosure or modification when communicated or stored.

12.3.2.4 OSP.ISSUANCE

OE.ISSUANCE is used to help OE.MANAGE as it pertains to the proper management of the TOE. For this Organizational Security Policy, the defined and enforced policy that governs identification and authentication requirements informs the administration of the TOE.

O.PHYSICAL_INTEGRITY The VeroCard case is tamper evident. Tampering attempts on the VeroCard trigger zeroization.

12.3.2.5 OSP.HANDLING

Users of the TOE as it pertains to the VeroCard and DocuSign HSM should be aware of its use and what results in tripping the tamper mechanisms as communicated by O.PHYSICAL_INTEGRITY and handles the VeroCard in accordance with OE.HANDLING.

OE.MANAGE should enforce this with proper administration, training, and guidance, for example so a user might be aware of what might be required of them such as what is laid out in OE.PHYSICAL.

O.PHYSICAL_INTEGRITY The VeroCard case is tamper evident. Tampering attempts on the VeroCard trigger zeroization.

12.3.2.6 OSP.PASSWORD_QUALITY

OE.MANAGE should provide appropriate guidance as to the configuration of password policies as users themselves should likewise be aware.

O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be contemporaneous: This part of data integrity means organizations should know how data appeared in its initial state and what happened to it throughout the different stages of its lifecycle.

12.3.2.7 OSP.PASSWORD_VALIDITY_PERIOD

OE.MANAGE should provide appropriate guidance as to the configuration of password policies as users themselves should likewise be aware.

O.DATA_INTEGRITY Use of the TOE for authentication and authorisation shall be contemporaneous: This part of data integrity means organizations should know how data appeared in its initial state and what happened to it throughout the different stages of its lifecycle.

12.3.3 Assumptions Tracing to Security Objectives and Security Objectives of the TOE environment rationale

12.3.3.1 A.LOCATE

OE.MANAGE has an assumption that appropriate guidance or instruction is given on where the TOE should be appropriately installed and located.

12.3.3.2 A.MANAGE

Proper management is key as OE.ISSUANCE, OE.HANDLING, OE.MANAGE, OE.PHYSICAL, OE.PROTECT, OE.USERS all deal with proper treatment of the TOE components as it applies in terms of compliance to laws, requirements, and guidance necessary.

12.3.3.3 A.NOEVIL

OE.ISSUANCE has an audit component which should aid in incentivising appropriate diligence that guards against wilful negligence.

OE.MANAGE it's assumed that administrators are properly trained and provided with enough guidance to properly use the TOE.

OE.PROTECT is appropriate because it has to do with administrators and the protection of the TOE.

OE.USERS are expected to use the VeroCard appropriately so that no unnecessary issues are caused.

12.3.3.4 A.PLATFORM

OE.MANAGE assumes that all those administrators and users using the platform that the TOE will be deployed in is properly configured and secured.

OE.PCB_AUTH assumes the VMS manufacturing process that erases all executables and data on the components mounted on the VeroCard PCB Board and the VeroCard is loaded with known authentic versions.

13 Extended Component Definition (ASE_ECD)

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The definition of FPT_EMS is in accordance with the definition of FPT_EMS for the family of Secure Signature-Creation Device Protection Profiles. Statements in the security target regarding TOE Emanation are only relevant to the VeroCard and the DocuSign HSM.

The TOE shall prevent attacks against sensitive data within the TOE control where the attack is based on external observable physical phenomena of the device. Examples of such attacks are evaluation of device's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover TOE emanation.

13.1 FPT_EMS TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

13.1.1 Component Levelling

FPT_EMS.1 TOE Emanation has two constituents:

- FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data; and
- FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

13.1.2 Management

FPT_EMS.1 There are no management activities foreseen.

13.1.3 Audit

FPT_EMS.1 There are no actions identified that shall be auditable if FAU_GEN (Security audit data generation) is included in an ST using FPT_EMS.1.

FPT_EMS TOE Emanation

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1 The TOE shall not emit ***[assignment: types of emissions]*** in excess of ***[assignment: specified limits]*** enabling access to ***[assignment: list of types of TSF data]*** and ***[assignment: list of types of user data]***.

FPT_EMS.1.2 The TSF shall ensure ***[assignment: type of users]*** are unable to use the following interface ***[assignment: type of connection]*** to gain access to ***[assignment: list of types of TSF data]*** and ***[assignment: list of types of user data]***.

14 Security Requirements (ASE_REQ)

This section defines the security requirements for the TOE. The security functional requirements are defined with reference to CC Part 2 and to Sect. 6. The security assurance requirements are defined with reference to a well-defined evaluation assurance package EAL2 Augmented with ALC_FLR.1 as defined in CC Part 3.

The statement of security functional requirements utilizes operations as defined for each applicable security functional requirement in CC Part 2 and Sect. 6. The notation for identifying the operations is as follows:

Iteration is identified by repeating the identifier of the security functional requirement with a string indicating a specific iteration separated from the security functional requirement (SFR) identification by a slash (e.g. FCS_COP.1/AES, FCS_COP.1/DSIG).

Refinement is identified by a) indicating in square brackets in bold font any added text, in form of [Refinement: added text] and b) indicating any removed words using overstrike font. Whenever a refinement is used, the rationale and justification of the refinement is given immediately after the statement of the security requirement.

Selection is identified by indicating the selected values in **[square brackets using bold font].**

Assignment is identified by indicating the assigned values in ***[square brackets using bold, italic font].***

Application notes may be added after the formal statement of the security requirements to assist the reader in understanding the specific security requirement in the context of this TOE Environment.

14.1 Statement of Security Functional Requirements

14.1.1 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic Support

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[*Advanced Encryption Standard (AES)*]** and specified cryptographic key sizes **[*128 bits*]** that meet the following: **[*FIPS PUB 197*]**.

FCS_CKM.2.1/DUKPT The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[*Derived Unique Key Per Transaction (DUKPT)*]** that meets the following: **[*ANSI X9.24 part 1*].**

FCS_CKM.2.1/ECDH The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method **[*Elliptic-curve Diffie-Hellman*]** that meets the following: **[*NIST SP 800-56A Rev. 3*].**

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[*zeroization*]** that meets the following:

[

DocuSign HSM: FIPS 140-2[3]; and

VeroCard: PCI PTS POI Modular Security Requirements A1[4]

].

FCS_COP.1 Cryptographic operation

FCS_COP.1.1/ECC256 The TSF shall perform **[*Firmware digital signature verification, Encryption of Key initialisation messages*]** in accordance with a specified cryptographic algorithm **[*Elliptic Curve Digital Signature Algorithm (ECDSA) and cryptographic curve algorithm NIST P-256*]** and cryptographic keys sizes **[*256 bits*]** that meet the following: **[*FIPS PUB 186-4*].**

FCS_COP.1.1/SHA-256 The TSF shall perform **[**

Production DocuSign HSM and VeroCard: ***Stored PIN-digest computation, Comparison PIN-digest computation; and***

Manufacturing and Production DocuSign HSM: TLS1.2 communication with c*ypher TLS_RSA_WITH_AES_256_CBC_SHA256*

] in accordance with a specified cryptographic algorithm **[*Secure Hash Algorithm 2 with 256 digest size*]** and cryptographic key sizes **[*256 bits*]** that meet the following**: [*FIPS PUB 180-4*].**

FCS_COP.1.1/AES The TSF shall perform **[*Key table encryption and decryption, DUKPT key material decryption, TOE Software encryption and decryption*]** in accordance with a specified cryptographic algorithm **[*Advanced Encryption Standard (AES)]*** and cryptographic key sizes ***[128 bits]*** that meet the following: **[*FIPS PUB 197*].**

[3] Applicable to both manufacturing and production DocuSign HSM hardware
[4] https://www.pcisecuritystandards.org/documents/PCI_PTS_POI_SRs_v4-1c-November.pdf November 2015

14.1.2 Class FDP: User Data Protection

FDP_ACC.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the **[*Key Import SFP*]** on **[*Subjects: TSF Objects: Cryptographic Keys Operations: Importing*]**.

FDP_ACF.1 Security attribute-based access control

FDP_ACF.1.1 The TSF shall enforce the **[*Key Import SFP*]** to objects based on the following**: [*TSF: Keyloaded*].**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[*Importing of Cryptographic Keys is only allowed when the Keyloaded state of the TSF is NOT set*].**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[**

In accordance with statements in the documents QSG_CC_001 Admin Quick Start Guide- Bootstrap process, ADG_CC_001 VeroGuard HSM Digital ID Solution Admin Guide sections 8.3 to 8.5 and AGD_OPE

- ***System Administrators can create new TOE operator users***
- ***Production DocuSign HSM users start, stop, and maintain only that device***
- ***VeroDataSource can edit the details of the SQL connection for terminal management system***
- ***VeroTmsView can view details in the terminal management system***
- ***VeroTmsAdmin and VeroTmsUser users can modify VeroCard records in the terminal management system***
- ***TMS Fallback User can log in as a VeroCard user for troubleshooting***
- ***Admin Portal Users BoID.Admin, BoID.Manager, BoID.Support can change the authorised resources for the VeroCard user***
- ***VeroSystemLog and VeroSystemConfig can view and configure VeroGuard console viewer***
- ***VeroCard User can be authenticated then authorised to access resources, plus change user PIN; and***
- ***VeroCard User can change the PIN stored on the VeroCard for offline verification***

].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[**

- ***On tamper detection by the VeroCard, authentication with the VeroCard will be denied***
- ***A VeroCard that has exceeded its PIN retry attempts will deny authentication***
- ***A VeroCard that is inactive in the Terminal Management System will deny online authentication; and***
- ***A VeroCard that is inactive in the Admin Portal will deny authorisation***

]

FDP_ITC.2 Import of User Data with Security Attributes

FDP_ITC.2.1 The TSF shall enforce the **[*Key Import SFP*]** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[For the VeroCard: *PIN minimum and maximum length*]**.

FDP_RIP.1 Residual Information Protection

FDP_RIP.1.1/PCB_SW The TSF shall ensure that any previous information content of a resource is made unavailable upon the **[*allocation of the resource to*]** the following objects: **[*Software on PCB mounted components*]**.

FDP_RIP.1.1/Keyloader 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: **[*Keyloader software*]**.

FDP_RIP.1.1/PIN 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: **[*PIN entered by the user*]**.

14.1.3 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when **[*Three (3)*]** unsuccessful authentication attempts occur related to **[*Online PIN verification and Offline PIN verification*]**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **[met]**, the TSF shall **[*cease authentication and display retry exceedance message*]**.

FIA_SOS.2 TSF Generation of Secrets

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet **[*Randomness criteria defined in NIST SP 800-90*].**

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for **[*Activation message replay prevention*].**

FIA_UAU.1 Timing of Authentication

FIA_UAU.1.1 The TSF shall allow **[*Establishment of Bluetooth connection, Authentication of the VeroCard*]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only **[*display of each entered PIN digit as an asterisk symbol*]** to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow [***for the VeroCard only***

- ***Firmware version check***
- ***Keyboard Beep on/off***
- ***Backlight brightness change and idle time power off time***
- ***Lifecycle state check (waiting for activation or activated); and***
- ***Power on/off***

] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

14.1.4 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[*Key Import SFP*]** to restrict the ability to **[change the default, modify or delete, or [*none*]]** the security attributes [***cryptographic keys or lifecycle state]*** to **[*no user roles (none)*]**.

FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the **[*Key Import SFP*]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **[*none*]** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[**

Management functions available during the manufacturing of the VeroCard:

- ***Removal of the bootloader software***
- ***Uploading of the bootloader software***
- ***Changing the security flags to disable bootloader erase and backdoor login***
- ***Uploading of the keyloader software***
- ***Identification of the supported commands***
- ***Identification of the integrated circuit (IC)***
- ***Identification of the VeroCard through serial number***
- ***Uploading cryptographic keys***
- ***Restoring default settings***
- ***Removal of the keyloader software; and***
- ***Locking the keys and setting the life-cycle state to Keyloaded.***

Management functions available in the Operational life-cycle stage:

- ***Verification of the software versions***
- ***Upgrading the Bluetooth driver software***
- ***Upgrading the VeroCard software***
- ***Setting the period after which a PIN is requested***
- ***Triggering the self-testing of the VeroCard components***
- ***Setting of the PIN for the user***
- ***Pairing with a Bluetooth device***
- ***Setting display brightness; and***
- ***Setting time before automatic powering off.***

].

FMT_SMR.1 The TSF shall maintain the roles [

- ***System Administrators***
- ***Production DocuSign HSM users start, stop, and maintain only that device***

- ***VeroDataSource, VeroTmsAdmin, VeroTmsUser, and VeroTmsView users***
- ***TMS Fallback User***
- ***Admin Portal users - BoID.Admin, BoID.Manager, BoID.Support***
- ***VeroSystemLog and VeroSystemConfig; and***
- ***VeroCard user.***

].

14.1.5 Class FPT: Protection of the TSF

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit **[*information about TOE power consumption, command execution time, keypad, or display*]** in excess of **[*information not usable for successful deduction or re-generation of secrets*]** enabling access to **[*cryptographic keys*]** and **[*PIN code*].**

FPT_EMS.1.2 The TSF shall ensure **[*users*]** are unable to use the following interface ***[Bluetooth connection, TOE surface, keypad, or display]*** to gain access to **[*cryptographic keys, life-cycle state*]** and **[*PIN code*].**

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: ***[attempted physical tampering, attempted logical tampering].***

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.

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to Physical Attack

FPT_PHP.3.1 The TSF shall resist **[**

VeroCard and DocuSign HSM: physical probing;

VeroCard only: exposure of unusual light, exposure of unusual temperature

] to the **[*TOE electrical components and memories*]** by responding automatically such that the SFRs are always enforced.

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **[*Cryptographic keys, PKI certificates*]** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use **[*Rules coded in the API calls used in the keyloading*]** when interpreting the TSF data from another trusted IT product.

FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self tests **[during initial start-up, at the request of the authorised user]** to demonstrate the correct operation of

[

For the VeroCard: Power On Self Tests (POST) including secure memory verification; and

For the DocuSign HSM: FIPS 140-2 Known Answer Tests (KATs) in the security policy document[5]

].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of

[

VeroCard: Bootloader software, Application software, Bluetooth driver software

].

[5] DocuSign 5.0 Security Policy Document 140sp2860, DocuSign 2018, https://csrc.nist.gov/CSRC/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2860.pdf

14.1.6 Class FTP: Trusted Paths/Channels

FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 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 The TSF shall permit **[the TSF]** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **[**

Keyloader communicating to the manufacturing DocuSign HSM for VeroCard key loading; and

Decrypting the following request created by the VeroCard then routed via VeroGuard.HSM.Host.DLL to the production DocuSign HSM:

- ***Device activation***
- ***Change PIN***
- ***Set PIN; and***
- ***Verify PIN***

].

14.2 Security Assurance Requirements

Security assurance requirements for the VeroCard constitute the evaluation assurance package EAL2 augmented with ALC_FLR.1 fully defined with reference to CC Part 3.

14.3 Security Requirements Rationale

14.3.1 Security Requirement Dependency Rationale

Each dependency of SFRs defined for the TOE is satisfied by the TOE. The satisfaction of dependencies appears below.

SFR	Dependencies	Justification
FCS_CKM.1	[FCS_CKM.2, or FCS_COP.1] FCS_CKM.4	FCS_COP.1 by the TOE. FCS_CKM.4 by the TOE.
FCS_CKM.2/DUKPT	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.2 by the TOE. FCS_CKM.4 by the TOE.
FCS_CKM.2/ECDH	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.1 by the TOE. FCS_CKM.4 by the TOE.
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or	FDP_ITC.2 by the TOE. FCS_CKM.1 by the TOE.

	FCS_CKM.1]	
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.2 by the TOE for the keys used for protecting the PIN codes and FCS_CKM.1 for the keys used for protecting the firmware stored in the memories outside of the integrated circuit (IC). FCS_CKM.4 by the TOE.
FCS_COP.1/ECC256	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FDP_ITC.2 by the TOE. FCS_CKM.4 by the TOE.
FCS_COP.1/SHA-256	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	None of the dependencies is applicable as cryptographic hash functions use no cryptographic keys.
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1 by the TOE
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 by the TOE FMT_MSA.3 by the TOE
FDP_ITC.2	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	FDP_ACC.1 by the TOE FTP_ITC.1 by the TOE FPT_TDC.1 by the TOE
FDP_RIP.1/PCB_SW	No dependencies	No dependencies
FDP_RIP.1/Keyloader	No dependencies	No dependencies
FDP_RIP.1/PIN	No dependencies	No dependencies
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1 by the TOE
FIA_SOS.2	No dependencies	No dependencies
FIA_UAU.1	FIA_UID.1	FIA_UID.1 is fulfilled by a required Bluetooth connection from the host prior to using the VeroCard.
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1 by the TOE
FIA_UID.1	No dependencies	No dependencies
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 by the TOE FMT_SMR.1 by the TOE FMT_SMF.1 by the TOE
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 by the TOE FMT_SMR.1 by the TOE
FMT_SMF.1	No dependencies	No dependencies
FMT_SMR.1	FIA_UID.1	FIA_UID.1 by the TOE
FPT_EMS.1	No dependencies	No dependencies
FPT_FLS.1	No dependencies	No dependencies
FPT_ITC.1	No dependencies	No dependencies
FPT_PHP.1	No dependencies	No dependencies

FPT_PHP.3	No dependencies	No dependencies
FPT_STM.1	No dependencies	No dependencies
FPT_TDC.1	No dependencies	No dependencies
FPT_TST.1	No dependencies	No dependencies
FTP_ITC.1	No dependencies	No dependencies

Table 9: Security Functional Requirement dependencies

14.3.2 Tracing of Security Objectives to Security Functional Requirements

The tracing of security objectives to the security functional requirements appears below.

SFR	O.PCB_AUTH	O.MANAGEMENT	O.EMSEC	O.PHYSICAL_INTEGRITY	O.DATA_INTEGRITY	O.PIN_PROTECTION
FCS_CKM.1					x	
FCS_CKM.2/DUKPT						X
FCS_CKM.2/ECDH						X
FCS_CKM.4						X
FCS_COP.1/ECC256					X	X
FCS_COP.1/AES					X	
FCS_COP.1/SHA256					X	X
FDP_ACC.1		X			X	
FDP_ACF.1		X			X	
FDP_ITC.2					X	
FDP_RIP.1/PCB_SW	X					
FDP_RIP.1/Keyloader		X			X	
FDP_RIP.1/PIN						X
FIA_AFL.1					X	
FIA_SOS.2					X	
FIA_UAU.1		X				
FIA_UAU.7		X				
FIA_UID.1		X				
FMT_MSA.1		X				
FMT_MSA.3		X			X	
FMT_SMF.1		X			X	
FMT_SMR.1		X			X	
FPT_EMS.1			X			
FPT_FLS.1					X	
FPT_ITC.1		X			X	
FPT_PHP.1			X	X		
FPT_PHP.3			X	X		
FPT_STM.1		X				
FPT_TDC.1					X	
FPT_TST.1		X				
FTP_ITC.1					X	

Table 10: Tracing of security objectives to Security Functional Requirements

14.4 Justification for the Security Assurance Requirements

The Security Assurance Requirements selected for the TOE constitute a well-defined evaluation assurance package EAL2 and as such, are an internally consistent set of security assurance requirements. EAL2 is augmented with Basic flaw remediation (ALC_FLR.1) as the VeroCard is a physical device issued in large quantities and cannot be easily recalled and reissued to address any software errors. Therefore, the VeroCard implements a mechanism to allow updating of the software if required.

Detailed statements that justify the mapping of SFRs to security objectives appear against each objective.

15 TOE Summary Specification (TSS)

This section describes:

- Keyloading Software Authenticity
- Offline Pin Verification
- Key Loading Assumption
- Activation
- Protecting the PIN codes in communication
- Physical Security of the TOE; and
- Protection of the TOE Software and Data

15.1 Keyloading Software Authenticity

Prior to the commencement of the keyloading, the VeroCard erases the existing bootloader and keyloading software from the VeroCard (FDP_RIP.1/PCB_SW). This removes the risk of software residing on the components mounted on the PCB during the manufacturing being tampered with prior to being received by the VeroCard manufacturing facility.

The VeroCard implements a management interface which allows erasure and uploading of the bootloader and keyloader software (FMT_SMF.1). The manufacturing system overwrites the existing software with known good versions of the keyloader and bootloader prior to the commencement of the keyloading. The loading of the cryptographic keys occurs by the manufacturing DocuSign HSM in a secure manufacturing facility over a secure Bluetooth connection (FTP_ITC.1).

15.2 Offline Pin Verification

The VeroCard can be used in off-line mode for authenticating to the Windows Operating System (OS) running on the PC to which the VeroCard is connected to via Bluetooth. In the scenario, the user attempts to login using the VeroCard while unable to communicate to VeroGuard which triggers the offline PIN verification. To ensure that the off-line PIN verification is secure, the VeroCard may establish a Bluetooth connection with the PC prior to the authentication and the communication between the VeroCard and the PC takes place over a secure Bluetooth connection (FIA_UAU.1, FTP_ITC.1).

A SHA-256 value of the user's PIN code (a PIN hash) is stored within the VeroCard (FCS_COP.1/SHA-256). The TOE also maintains a 'Successful PIN' register and a retry-counter in the SQL database. The PIN retry counter is set to three which allows three attempts for the user to enter the PIN. If each attempt is unsuccessful, the VeroCard erases the reference PIN hash stored within and only can be used for online verification (FIA_AFL.1).

The PIN, when entered into the VeroCard by the user, is only displayed as asterisk symbols (FIA_UAU.7) and stored in a temporary value register. Upon completion of the PIN entry, the PIN is hashed (FCS_COP.1/SHA-256) and the temporary register cleared (FDP_RIP.1/PIN). The computed PIN value digest is compared to the digest of a reference PIN value stored on the VeroCard. If the values match,

the 'Successful PIN' register is set to a positive value, the PIN retry counter reset and the outcome communicated to the PC. Otherwise, the value of the PIN retry counter is deducted by one. If the value has reached zero, the VeroCard erases the locally stored reference PIN hash (FIA_AFL.1). Otherwise, the user is prompted to re-enter the PIN and the verification process is re-executed.

15.3 Key Loading

Initial cryptographic keys used by the VeroCard are loaded during the manufacturing. The loading occurs within a secure manufacturing facility using a physically and logically secure key loading devices where the instances of VeroCard are handled robotically and moved to a Faraday cage in which a dedicated Key loader connected to the production DocuSign HSM performs the key loading.

If at any time during the key loading process a step, test or validation fails, the key loading process is aborted, the error details are logged in the manufacturing database, the production control system is informed of a failure, the failure is logged, the fail light is illuminated. The VeroCard in which the step failed is ejected on the tray and the robotic arm moves the said VeroCard to a rework holding position. The device either becomes ready to re-attempt key loading if aborted at an early stage before tamper resistance features are enabled or enters a Tampered state and is scheduled to be investigated and/or destroyed.

The key loader service has an API key and a unique identifier that is generated from the hardware it is running on. The unique identifier is used by the key loader service to register itself with the manufacturing system. An administrator of the manufacturing system shall enable the key loader station to begin communicating with the key loading devices.

Prior to the key loading, the VeroCard is in a default state where the key loading is allowed (FMT_MSA.3). Only upon successful loading of the keys the key loading system request the VeroCard to lock the keys in which stage the key loading shall no longer be possible (FDP_ACC.1, FDP_ACF.1). As the VeroCard has no identified and authenticated users, the VeroCard maintains no roles and there exists no user who is authorised to change the default values and prevent the keyloading from occurring (FMT_MSA.1). There are also no management functions which would allow this (FMT_SMF.1). Upon completion of the key loading shall the manufacturing system request the VeroCard to lock the keys which transfers the VeroCard to the Keyloaded state and prevents re-loading of the keys from occurring.

Refer to the document SPC_CC_004 VeroCard Key Loading Design & Implementation section 4: “Key Loading Process” for a detailed description of where and how the manufacturing DocuSign HSM, keyloader and VeroCard use public and private keys. Steps to complete key loading below are taken from that document:

Once the VeroCard receives keys from the manufacturing DocuSign HSM, they are stored AES-CBC encrypted using the 128-bit AES key constructed from KEK received in two parts (FCS_COP.1/AES).

The key loader service starts scanning for Bluetooth Low Energy (BLE) advertisements, filtered by the Bluetooth MAC Address that it obtained in the previous step. If no matching device is found after 30 seconds it will retry for a total of 3 times before reporting back to the manufacturing service that no

device matching the MAC Address was found. If a matching device is found, the keyloader and the VeroCard establishing a secure Bluetooth Mode 1 Level 4 connection. All subsequent communication for key loading takes place over that secure connection (FTP_ITC.1).

Once connected, a command is sent to the VeroCard to identify the API calls it supports for keyloading (FMT_SMF.1, FPT_TDC.1.2). If the required API is available, a command is sent to the card to request for the ID of the IC and Serial Number of the device. These are checked against the values returned by the manufacturing service earlier. If they are correct, the manufacturing continues if they match. Otherwise, the device is rejected (FMT_SMF.1).

The VeroCard is asked for the version of firmware that is installed which is checked against the version returned earlier from the manufacturing service to ensure that keys are loaded using expected version of software (FMT_SMF.1).

The VMS establishes a session to the manufacturing DocuSign HSM encrypted with TLS1.2 (FPT_ITC.1.1) and the available keys are made available for the keyloader.

Once the session is established, the actual loading of the keys to the VeroCard commences. All communication between the VeroCard and the Keyloader takes place over a secure Bluetooth Mode 1 Level 4 connection (FTP_ITC.1.1).

Terminal Keys are generated by the manufacturing DocuSign HSM and sent to the VeroCard. These keys include the following:

Name	Definition
KEK Part 1	128-bit symmetric key
KEK Part 2	128-bit symmetric key
RNG key	192-bit symmetric key
RAND	128-bit symmetric key

Table 11: Terminal Keys

Key Encryption Key (KEK) Part 2 is stored by the VeroCard but not used. Random Number Generator (RNG) and RAND are only for the legacy purposes and are neither stored nor used by the VeroCard. Only KEK Part 1 is used as a Key Encryption Key.

Local time is then sent to the VeroCard.

A 256-bit ECDSA key pair is generated by the manufacturing DocuSign HSM and sent to the VeroCard (FDP_ITC.2). The key components are encrypted with 128-bit AES in CBC mode using the KEK generated from KEK Part 1 (FDP_ITC.2, FCS_COP.1/AES).

Using the 256-bit ECDSA Public Key that was just generated, a SHA256 digest of the public key is computed (FCS_COP.1/SHA-256) and passed to the manufacturing DocuSign HSM along with the name of the ManufacturerPrivateKey to generate a signature of the key which is then sent to the VeroCard(FPT_TDC.1.1).

The following keys are generated by the manufacturing DocuSign HSM and exported to the VeroCard (FDP_ITC.2, FPT_TDC.1.1):

- A 256-bit ECDSA Manufacturer Public Key
- A 256-bit ECDSA GatewayPublicSigningKey; and
- A 256-bit ECDSA ManufacturerPublicKey.

The two commands are sent to the VeroCard (FMT_SMF.1):

- A command to restore default settings; and
- A command to verify that the ID of the IC and Serial Number are still correct and have not changed.

If everything is successful to this point, a command is sent to the VeroCard to lock all the keys. The locking transfers the KeyLoaded state to the value YES which is interpreted as the keyloading being completed and the VeroCard being ready to move to the next life-cycle stage (FMT_SMF.1, FPT_TDC.1.2). The cryptographic keys cannot be loaded again once this stage is completed (FDP_ACC.1, FDP_ACF.1).

After locking the keys, a command is sent to the VeroCard to restart. When the device starts up it removes the key loader firmware (FDP_RIP.1.1/Keyloader) which is replaced by the main application firmware that had been previously loaded in the device at an earlier station (FMT_SMF.1).

The key loader disconnects from the VeroCard and starts scanning for BLE advertisements, again filtered by the Bluetooth MAC Address, and it waits until the device is visible again and connects. Once connected, a command is then sent to the VeroCard to ask it for its current state, and if everything was successful the expected return value is “Ready to Activate”.

The key loader service finally posts an API call to the manufacturing service with the result of the key loader process (successful or failed with detailed status code) and the faraday cage is lifted and the VeroCard moves to the next station on the manufacturing line.

15.4 Activation

To protect the PIN codes when communicated to the production DocuSign HSM, the VeroCard engages in a Derived Unique Key Per Transaction (DUKPT) Remote Key Injection (RKI) protocol with the production DocuSign HSM to derive the secret key to be used for securing the subsequent communication between the VeroCard and the production DocuSign HSM (FPT_TDC.1.1).

The activation takes form of the VeroCard generating a key initialisation request message and sending it to the production DocuSign HSM. The VeroCard generates the message and encrypts it with the Manufacturer Public Key loaded to the VeroCard during the key loading (FCS_COP.1/ECC256). The message is padded with a time stamp (FPT_STM.1) and a random quantity (FIA_SOS.2) which prevent replay attacks of the activation exchange. As part of the activation message, the VeroCard engages in an elliptic-curve Diffie-Hellman exchange with the production DocuSign HSM to generate a 128-bit AES key (FCS_CKM.2/ECDH). That key is used for the production DocuSign HSM to return to the VeroCard the DUKPT protocol elements which can be decrypted by the VeroCard using the generated key (FCS_COP.1/AES).

15.5 Protecting the PIN Codes in Communication

Using the key material received from the production DocuSign HSM during the activation of the VeroCard, the VeroCard can engage in a DUKPT key derivation in synchrony with the backend HSM. The VeroCard generates DUKPT Future Keys (FCS_CKM.2/DUKPT) which are 128-bit AES keys. These keys are then used for encrypting the PIN blocks when sent to the production DocuSign HSM (FCS_COP.1/AES). Each Future Key is zeroized once used (FCS_CKM.4) but the VeroCard may generate fresh ones from the DUKPT keying material.

15.6 Physical Security of the TOE

The VeroCard is a physical device used in a potentially hostile environment. Consequently, it is engineered to prevent exposure of the secrets stored on it or modification of software or data through physical breach of the device security measures.

The VeroCard casing is unopenable and any attempt of physical tampering shall leave obvious traces which can be easily detected by visual detection of the device (FPT_PHP.1). The VeroCard also actively monitors the physical integrity and in case of physical probing being detected, triggers defensive measures as described below (FPT_PHP.3).

The VeroCard PCB is wrapped in a mesh which is connected to the secure IC circuitry. In case of physical probing, disturbing the IC circuitry triggers protective measures. These measures include zeroization. These claims are in accordance with typical payment card industry certification requirements.

Furthermore, the physical casing of the VeroCard and the mesh around the PCB of the VeroCard control electromagnetic emanations. The emanation control mechanisms ensure that any emanations from the device do not contain enough information to deduce the secrets used by VeroCard for various computations or to allow cloning of the TOE (FPT_EMS.1). Obviously, the NFC and Bluetooth antennas and the inductive charging circuit are outside of the security mesh controlling emanations to allow communication and charging of the VeroCard.

Each DocuSign HSM is tamper-evident and has a comprehensive suite of tamper protection which includes tamper-detection and zeroization.

15.7 Protection of the TOE Software and Data

The VeroCard contains two main types of memories: the secure memory of the IC and the on-PCB memory. Software of the VeroCard resides in both. Additionally, the Bluetooth chip contains the Bluetooth driver software.

Executables residing on the VeroCard PCB received from the manufacturer are erased during manufacturing (FDP_RIP.1/PCB_SW) and replaced by known, authentic versions to ensure that the keyloading occurs on authentic software. The replacement occurs over a secured Bluetooth connection (FTP_ITC.1) and (FMT_SMF.1). The manufacturer may send the operator a new VeroCard executable

which the operator may choose to install. The installation of the new executable is in accordance with the document ADG_CC_001 VeroGuard HSM Digital ID Solution Admin Guide (FMT_SMF.1).

Software not stored within the secure memories of the IC is stored on the PCB-mounted Flash. When the VeroCard is initialised, a 128-bit AES key is generated for encrypting the software (FCS_CKM.1). That key is then used for encrypting all software stored in the Flash and for decrypting the software only when fetched for execution (FCS_COP.1/AES).

In the VMS, information transferred between the keyloader and the manufacturing DocuSign HSM is encrypted using TLS1.2 (FPT_ITC.1.1). Messages that are encrypted and sent from or to the VeroCard by the TOE component VeroGuard.HSM.Host.DLL are passed to the production DocuSign HSM by VeroGuard.HSM.Host.DLL encrypted with TLS1.2 (FPT_ITC.1.1).

The software and data are stored in various memories and registers of the VeroCard and protected by the following mechanisms:

- At the start-up, the VeroCard runs a suite of self-tests to ensure that the software is authentic (FPT_TST.1)
- All cryptographic keys are stored in secure registers of the IC. Once they are loaded during the manufacturing, the VeroCard enters a life-cycle state Keyloaded where reloading of the same keys may no longer occur (FDP_ACC.1, FDP_ACF.1)
- The reference PIN code is not stored in a recoverable format but a SHA-256 digest of it is stored for off-line verification (FCS_COP.1/SHA-256)
- The user entered PIN is stored in a temporary register and erased immediately after being hashed for off-line verification or encrypted for forwarding to the production DocuSign HSM for verification (FDP_RIP.1.1/PIN)
- When being entered, the PIN digits are obfuscated to ensure that anybody observing the display of the VeroCard while the PIN is being entered shall not learn the PIN (FIA_UAU.7)
- If the VeroCard detects any attempted logical or physical tampering, it triggers a secure state in which the attack is mitigated as the sensitive data is erased and the VeroCard entered to the Tampered state (FPT_FLS.1)
- Only the menu functions of the VeroCard are available to the user prior to authentication with a PIN (FIA_UID.1). Once the user has authenticated with the VeroCard or the administration console, authorisation is governed by roles-based access control (FMT_SMR.1); and
- If the manufacturing or production DocuSign HSM detects any attempted logical or physical tampering, it triggers a secure state in which the attack is mitigated as the sensitive data is erased and the manufacturing or production DocuSign HSM enters the Tampered state (FPT_FLS.1)

