Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

VeroGuard HSM Digital ID for Open Networks V1.0

Version 1.0, 10 February 2022

cyber.gov.au

ACSC Australian Cyber Security Centre

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of VeroGuard HSM Digital ID for Open Networks V1.0 against Common Criteria EAL2+ALC_FLR.1.

The Target of Evaluation (TOE) is VeroGuard HSM Digital ID for Open Networks V1.0. The TOE provides a handheld Hardware Security Module (HSM) with a PIN Entry Device (PED) and the VeroGuard Identity platform with its own HSM. The VeroGuard Identity platform authenticates PIN validation attempts generated from the VeroCard. The TOE uses a Bluetooth link to support two main use cases:

- secure access to Bluetooth enabled Windows machine desktops without a password
- secure access to websites and applications from Bluetooth enabled browsers.

This report concludes that the TOE has complied with the Common Criteria (CC) Evaluation Assurance Level EAL2 augmented with ALC_FLR.1 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP).

Common Criteria Guidance is available in the *VeroGuard HSM Digital ID Solution Admin Guide* [5] delivered with the rest of the TOE from VeroGuard.

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program. The evaluation was performed by DXC Australia's Australian Information Security Evaluation Facility (AISEF) and was completed on 13 January 2022.

With regard to the secure operation of the TOE, the Australian Certification Authority (ACA) recommends that:

- the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- users review their operational environment and ensure security objectives for the operational environment can be met
- users configure and operate the TOE according to the *VeroGuard HSM Digital ID Solution Admin Guide*
- users make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- the passwords and PINs for all identities should be handled securely
- users should verify the integrity of the TOE software prior to installation by comparing the delivered TOE Components with the TOE Component SHA-256 hashes in the *Verification of Delivered Solution Configuration* [5] document available from VeroGuard
- resources used to implement the VeroGuard HSM Digital ID solution should be protected using techniques such as network segmentation to shield the server parts of the TOE from external network attack
- users are aware that the TOE use of a wireless link (Bluetooth Low Energy) between the VeroCard and the user computer that brings user benefits due to improved usability but introduces security risks in terms of availability and eavesdropping that should be considered.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target [6] and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [6] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is VeroGuard HSM Digital ID for Open Networks V1.0.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	VeroGuard HSM Digital ID for Open Networks
Product version	V1.0
Security Target	VeroGuard HSM Digital ID Security Target version 1.19 dated 03 February 2022
Evaluation Technical Report	VeroGuard HSM Digital ID for Open Networks Evaluation Technical Report 1.0 dated 04 February 2022 Document reference DXC-EFC-T092-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, Version 3.1 Rev 5, April 2017
Methodology	Common Methodology for Information Technology Security, Version 3.1 Rev 5, April 2017
Conformance	EAL 2 augmented with ALC_FLR.1 (Basic flaw remediation)

Developer	VeroGuard Systems Pty Ltd PO Box 5003 Clayton VIC 3168 Australia VeroGuard Certification Officer: certifications@veroguard.com.au
Evaluation facility	DXC Australia Pty Ltd 26 Talavera Road Macquarie Park NSW 2113 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is VeroGuard HSM Digital ID for Open Networks V1.0.

The VeroGuard HSM Digital ID solution provides multi factor authentication for open networks using encrypted data. The solution consists of a handheld HSM with a PIN Entry Device (PED) “the VeroCard” and the VeroGuard Identity platform with its own HSM. The VeroGuard Identity platform authenticates PIN validation attempts generated from the VeroCard. The solution is suitable for secure authentication across open networks such as the public internet. Authorisation of third-party applications is available through the VeroGuard Identity platform. Authorisation of Windows credentials is available through the VeroGuard Serenity Credential Manager, included in the TOE.

Possible applications of the TOE include:

- secure access to Windows and other desktops without a password
- secure access to web sites and applications from any Bluetooth enabled device.

TOE Functionality

The TOE functionality that was evaluated is listed below:

- cryptographic functions including the generation, distribution, use and destruction of cryptographic keys
- user data protection by role-based access controls
- identification and authentication
- security management
- enhanced protection of TOE security functions.

The above are described in more detail in Section 14.1 of the Security Target [6].

TOE physical boundary

The TOE physical boundary is described in section 9.4 of the Security Target [6].

TOE Architecture

The VeroGuard HSM Digital ID solution relies on:

- the VeroGuard Manufacturing System
- the VeroGuard HSM Digital ID for Open Networks production solution.

VeroGuard Manufacturing System activities occur at the VeroGuard manufacturing facilities and includes steps such as firmware installation and key injection.

The solution delivered to the user premises consists of any number of VeroCards that interact with properly enabled Microsoft Windows computers or suitable browsers to communicate with a backend production HSM using recent Payment Card Industry (PCI) technology.

In the Microsoft Windows Active Directory use case the Domain Controller is dynamically setup to allow network login from the VeroCard. In the Open ID connect (OAuth2) use case the browser is provided with the tokens needed for the allowed accesses.

The TOE also provides a richly featured management application to manage the VeroCards using the VeroGuard HSM Digital ID for Open Networks infrastructure.

Clarification of scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [6].

Non-evaluated functionality and services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [4] for policy relating to using an evaluated product in an unevaluated configuration.

Security

The TOE Security Policy is a set of rules that defines how information within the TOE is managed and protected. The Security Target [6] contains a summary of the evaluated functionality.

Usage

Evaluated configuration

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per operational guidance documentation [5].

Secure delivery

Hardware delivery procedures

Shipment of units from VeroGuard to the TOE Operator is via a commercial courier company who will pick up the TOE components from VeroGuard and deliver them directly to the user.

After placing an order, VeroGuard will issue an Order Acknowledgement Form listing the assigned user order number, the model number(s), serial number(s) and expected date of delivery. When items are received, the customer must ensure that the serial number on the outside of the packaging, the serial number attached to the TOE Hardware components and the number listed on the acknowledgement match.

Prior to delivery of the TOE hardware, VeroGuard and the TOE operator will exchange PGP keys to ensure secure transmission of images of tamper seals and the delivery-docket. The PGP keys may also be used for transmission of software updates.

The customer must also verify that tamper proof seals are intact and that the images of the seals provided by secure email match the detail of the delivered hardware. If the seal is broken, then the integrity of the TOE cannot be assured and VeroGuard should be informed immediately.

Software delivery procedures

Shipment of updated software is completed by encrypting any updated software TOE components along with instructions, using the PGP keys created as part of the delivery process. The encrypted attachment is delivered by email.

Installation of the TOE

The guidance documentation [5] contains all relevant information for the secure configuration of the TOE.

Version verification

VeroGuard HSM Digital ID for Open Networks V1.0 is a distributed system made of many components with various independent version numbers. This is made clear in Section 3 of the Security Target [6] reproduced below,

Hardware elements:

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

Software / Firmware elements:

- Keyloader 1.0.26
- VeroCard Firmware including Bluetooth driver VC0001xxxxxx
- DocuSign HSM Firmware 5.0.2
- Serenity Credential Provider 1.0.107.0
- VeroGuard.Tms.exe 1.0.860.1
- VeroBureau.Api.exe 1.3.148.1
- 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.

A document *Verification of Delivered Solution Configuration* [5] is available from VeroGuard containing procedures on how to check the version of each relevant TOE component.

Documentation and guidance

The TOE guidance documentation is in the *VeroGuard HSM Digital ID Solution Admin Guide* [5] document available from VeroGuard.

All Common Criteria material is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [4]

Secure usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met:

- individuals managing the TOE are competent and appropriately trained
- authorised administrators are not careless, wilfully negligent or hostile
- users have (and understand) comprehensive user manuals
- the manufacturing HSM and the production HSM and application servers will be located within controlled access facilities which prevent unauthorised physical access.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

Evaluation procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3* [1, 2].

Testing methodology was drawn from *Common Methodology for Information Technology Security, Version 3.1 Revision 5* [3].

The evaluation was carried out in accordance with the operational procedures of the Australian Information Security Evaluation Program [9].

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [8]* were also upheld.

Functional testing

To gain confidence that the developer testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining the test coverage, test plans and procedures, and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

These developer tests are designed in such a way as to exercise the TOE security functional requirements and the TOE interfaces identified in the TOE design documentation.

Penetration testing

The evaluator performed a vulnerability analysis of the TOE in order to identify any obvious security vulnerability in the product, and if identified, to show that the security vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible security vulnerabilities in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

- time taken to identify and exploit (elapsed time)
- specialist technical expertise required (specialist expertise)
- knowledge of the TOE design and operation (knowledge of the TOE)
- window of opportunity
- IT hardware/software or other equipment required for the exploitation.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

EAL2 provides assurance by a full security target and an analysis of the Security Functional Requirements (SFRs) in that security target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE Security Functionality (TSF), evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL1 by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain), and independent testing based upon more detailed TOE specifications.

Certification result

The DXC AISEF **has determined** that the TOE upholds the claims made in the Security Target [6] and **has met** the requirements of Common Criteria EAL2+ALC_FLR.1.

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [7], the Australian Certification Authority **certifies** the evaluation of VeroGuard HSM Digital ID for Open Networks V1.0 performed by the Australian Information Security Evaluation Facility, DXC AISEF.

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual* [4].

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

The Australian Certification Authority also recommends:

- that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- users review their operational environment and ensure security objectives for the operational environment can be met
- users configure and operate the TOE according to the *VeroGuard HSM Digital ID Solution Admin Guide* [5]
- users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings
- passwords and PINs for all identities should be handled securely
- users should verify the integrity of the TOE software prior to installation by comparing the SHA-256 hash of the delivered software against the value available in VeroGuard's *Verification of Delivered Solution Configuration* [5] document
- resources used to implement the VeroGuard HSM Digital ID solution should be protected using techniques such as network segmentation to shield the server parts of the TOE from external network attack
- users are aware that the TOE use of a wireless link (Bluetooth Low Energy) between the VeroCard and the user computer that brings user benefits due to improved usability but introduces security risks in terms of availability and eavesdropping that should be considered.

Annex A – References and abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components Version 3.1 Revision 5, April 2017*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components Version 3.1 Revision 5, April 2017*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 5, April 2017*
4. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
5. Guidance documentation:
   - *VeroGuard HSM Digital ID Solution Admin Guide (ADG_CC_001) v2.2, 21 December 2021*
   - *Verification of Delivered Solution Configuration* (ADG_CC_002) v1.7, 5 November 2021
   - *CC FAQ* - https://www.support.veroguard.com.au/cc-faq
6. *VeroGuard HSM Digital ID Security Target Version 1.19 dated 03 February 2022*
7. VeroGuard HSM Digital ID for Open Networks, Evaluation Technical Report, DXC-*EFC-T092-ETR 1.0 dated 04 February 2022*
8. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2-July-2014*
9. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf

Abbreviations

AISEP	Australian Information Security Evaluation Program
API	Application Programming Interface
ASD	Australian Signals Directorate
BLE	Bluetooth Low Energy
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
EAL	Evaluation Assurance Level
GPG	GNU Privacy Guard – PGP software
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
OAuth2	Open Authorization V2
PCI	Payment Card Industry
PED	PIN Entry Device
PGP	Open PGP Standard – RFC4880
SHA256	Secure Hash Algorithm 256 bit digest
TLS 1.2	Transport Layer Security version 1.2
TOE	Target of Evaluation
TSF	TOE Security Function
UI	User Interface