Certification Report

H1D3 Secure Microcontroller with Crypto Library v0.1.4

Sponsor and developer: ***Google LLC***
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

Evaluation facility: ***SGS Brightsight BV***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-0228971-CR**
Report version:	**2**
Project number:	**0228971**
Author(s):	**Hans-Gerd Albertsen**
Date:	**12 November 2021**
Number of pages:	**13**
Number of appendices:	**0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the H1D3 Secure Microcontroller with Crypto Library v0.1.4. The developer of the H1D3 Secure Microcontroller with Crypto Library v0.1.4 is Google LLC located in Mountain View, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a Secure Microcontroller with Crypto Library. The TOE is used in smartphone, servers and personal computers to increase the security of the platform including but not limited to secure boot, user authentication, and user data protection.

The H1D3 Secure Microcontrollers are provided in one of three packages referenced H1D3M, H1D3C and H1D3P. The Secure Microcontroller is a flash-based secure microcontroller platform. A RISC-V core named Soteria alongside RAM, ROM and flash memories and cryptographic hardware accelerators provides the root to run secure applications. The TOE includes a Crypto Library. The image loaded and verified by the TOE bootloader stored in ROM includes the Crypto Library in addition to the Embedded Software.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in section 3.2, 3.4, and 3.5 of the H1D3 User Guidance as referenced in the *[ST]*. As such it is vital that meticulous adherence to the user guidance of both the software and the hardware part of the TOE is maintained.

The TOE has been evaluated by SGS Brightsight BV located in Delft, The Netherlands. The evaluation was completed on 08 November 2021 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the H1D3 Secure Microcontroller with Crypto Library v0.1.4, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the H1D3 Secure Microcontroller with Crypto Library v0.1.4 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ATE_DPT.2 (Testing: security enforcing modules), ALC_DVS.2 (Sufficiency of security measures), and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the H1D3 Secure Microcontroller with Crypto Library v0.1.4 from Google LLC located in Mountain View, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	H1D3 Secure Microcontroller (packaged as H1D3M, H1D3P or H1D3C)	3
Software	Bootloader (embedded in ROM)	7f4bdb
	Crypto Library	0.1.4

To ensure secure usage a set of guidance documents is provided, together with the H1D3 Secure Microcontroller with Crypto Library v0.1.4. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 1.5.4.

2.2 Security Policy

The TOE maintains:

- the integrity and confidentiality of code and data stored in its memories as defined in the *[ST]*.
- the integrity, the correct operation and the confidentiality of security functionality provided by the TOE.

This is ensured by the construction of the TOE and its security functionality.

The H1D3 Secure Microcontroller with Crypto Library v0.1.4 basically provides the following hardware features:

- Memory Protection Unit (MPU)
- HMAC- SHA256, SHA256
- AES and TDES hardware engines
- Public Key cryptographic coprocessor
- A True Random Number Generator (TRNG)
- A Deterministic Random Bit Generator (DRGB) based on HMAC
- Environmental sensors.

In addition, the TOE provides the following software features as part of the IC Dedicated Software:

- Bootloader
- Cryptographic library, providing the following services or access to HW co-processors:
  - RSA signature verification
  - EC Key Generation
  - ECDSA
  - ECDH
  - AES (CBC, ECB, CMAC, GCM, and CRT)
  - TDES (CBC, ECB)
  - SHA256
  - HMAC SHA-256

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The TOE consists of the Secure Microcontroller hardware and the IC Dedicated Software.

The following hardware features are provided:

- RISC-V Soteria CPU with a single execution mode
- Memory Protection Unit (MPU)
- Flash memory with two banks (containing the same information for redundancy purpose)
- RAM memory
- ROM memory
- OTP memory (Fuse)
- HMAC-SHA256, SHA256, AES and TDES hardware engines
- Public Key cryptographic coprocessor
- A True Random Number Generator (TRNG)
- A Deterministic Random Bit Generator (DRBG) based on HMAC
- Environmental sensors

A block diagram is given in Figure 1 below.

The TOE's IC Dedicated Software comprises the bootloader and the Crypto Library. The bootloader is stored in ROM. The image loaded and verified by the TOE bootloader includes the Crypto Library in addition to the Embedded Software. The Crypto Library is described in section 2.2 above.

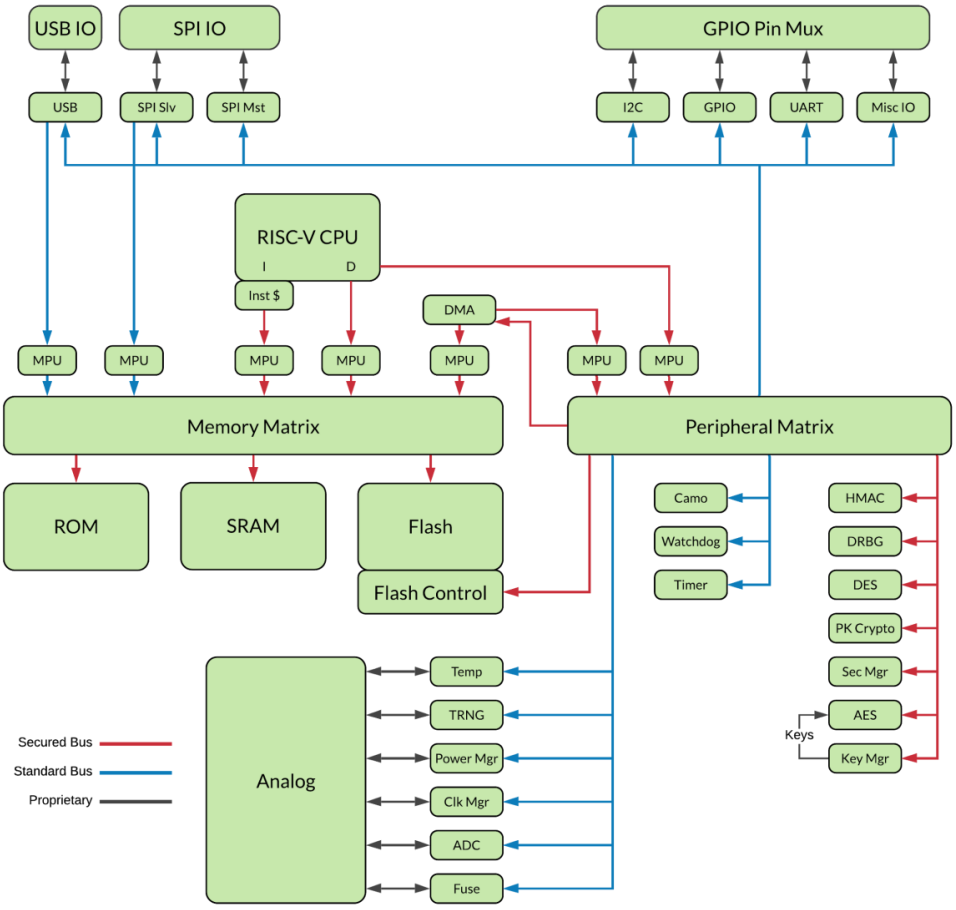

Figure 1. Logical architecture of the TOE.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version	
H1D3 Preparatory Guidance	1.3	2021-10-08
Cryptolib v0.1.4 API User Guidance	0.1.4	2021-06-15
Addendum Cryptolib v0.1.4 API User Guidance	1.4	2021-06-14
H1D3C Datasheet	1.2	2021-06-30
H1D3M Datasheet	1.2	2021-06-30
H1D3P Datasheet	1.2	2021-06-30
H1D3 Register Specification [2]		2021-09-30
H1D3 User Guidance	1.3	2021-09-28
H1D3 Code Signing	1.1	2021-09-28
H1D3 SPI flashing instructions	1.2	2021-10-08
Soteria Technical Reference Manual	1.3	2021-10-08

[2] The version of this document is linked to the TOE version '3'

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

For the hardware parts of the TOE, the developer performed three categories of testing: pre-silicon testing (simulation/emulation), post-silicon testing and production testing. These test categories are combined to achieve a good coverage and depth of testing, both on the design of the hardware parts of the TOE and on each of the manufactured ICs.

For the software parts of the TOE, the developer performed three categories of testing: simulation tests (including code coverage analysis), emulation and on-TOE testing. These categories were applied to the TOE to achieve a good coverage and depth of testing. All tests were executed using an automated framework.

The tests performed by the evaluator are selected focusing on the verification of security features, with a focus on functionality that cannot be covered with code coverage analysis (e.g. cryptographic operations). Repeating the tests requires the same equipment used by the developer, which is not always available at the ITSEF. Therefore, all selected tests were witnessed remotely at the developer's site.

All test results were as expected. No deviations were found.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE focused on the Secure IC, Cryptographic Library and Bootloader. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this, analysis will be performed taking into account the attack methods in *[JIL-AM]* and applicable attack papers with rating according to *[JIL-AAPS]*.
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 50 weeks. During that test campaign, 38% of the total time was spent on Perturbation attacks, 60% on side-channel testing, and 2% on logical tests.

2.6.3 Test configuration

The testing was performed on the TOE (H1D3) and on an earlier version of the TOE (H1D2). The differences between these two versions have been analysed. They have no impact on the test results; hence the test results of the earlier version apply also to the TOE. It should be noted that the hardware version also uniquely identifies the Bootloader, which is in ROM.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”. The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of two Site certificates and two Site Technical Audit Reuse reports.

Seven sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number H1D3 Secure Microcontroller with Crypto Library v0.1.4. The TOE can be identified as described in the H1D3 Preparatory Guidance as referenced in the *[ST]*. The hardware version can be read from a dedicated register, whereas the Crypto Library version can be determined from its commit hash through the provided API.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Reports for the audited sites[3], namely *[STAR MTV]*, *[STAR SVL], [STAR EAG], [STAR GDC],* and *[STAR TSMC Fab3].*

It should be noted that a sample of three out of twenty-eight data centres (selected by the scheme) were audited to demonstrate that consistent security measures are applied across all data centers. The result of the audits performed at the three data centres is documented in the single Site Technical Audit Report *[STAR GDC].*

To support composite evaluations according to *[COMP]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is “**Pass**”.

Based on the above evaluation results the evaluation lab concluded the H1D3 Secure Microcontroller with Crypto Library v0.1.4, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ATE_DPT.2, ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims ’strict’ conformance to the Protection Profile *[PP_0084]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE.

This TOE is critically dependent on the operational environment to provide countermeasures against specific attacks as described in section 3.2, 3.4, and 3.5 of the H1D3 User Guidance as referenced in the *[ST]*. Therefore, it is vital to maintain meticulous adherence to the user guidance of both the software and the hardware part of the TOE.

[3] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. To be protected against attackers with a “high attack potential”, appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The Titan H1D3 Secure Microcontroller with Crypto Library v0.1.4 Security Target, v2.4, 05 November 2021 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MITM	Man-in-the-Middle
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
TRNG	True Random Number Generator

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report "H1D3 Secure Microcontroller with Crypto Library v0.1.4" – EAL4+, 20-RPT-1236, v3.0, 08 November 2021
[ETRfC]	Evaluation Technical Report for Composition "H1D3 Secure Microcontroller with Crypto Library v0.1.4" – EAL4+, 21-RPT-1028, v3.0, 08 November 2021
[JIL-AM]	Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)
[JIL-AAPS]	JIL, (Mandatory) Application of Attack Potential to Smartcards, Version 3.1, June 2020
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP_0084]	Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014
[ST]	Titan H1D3 Secure Microcontroller with Crypto Library v0.1.4 Security Target, v2.4, 05 November 2021
[ST-lite]	Titan H1D3 Secure Microcontroller with Crypto Library v0.1.4 Security Target Lite, v2.4, 05 November 2021
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR MTV]	Site Technical Audit Report – Mountain View (MTV)-2015, 21-RPT-430, v3.0, 23 August 2021
[STAR SVL]	Site Technical Audit Report – Google Sunnyvale TC1, 21-RPT-431, v2.0, 30 June 2021
[STAR EAG]	Site Technical Audit Report – EAG Santa Clara, 21-RPT-429, v2.0, 30 June 2021
[STAR GDC]	Site Technical Audit Report – Google Data Centres, 21-RPT-986, v3.0, 28 October 2021
[STAR TSMC Fab3]	Site Technical Audit Report – TSMC Fab3, 21-RPT-1080, v2.0, 28 October 2021

(This is the end of this report.)