Certification Report

NVIDIA DRIVE OS Virtualization Software v6.0.9.3.1

Sponsor and developer: ***NVIDIA Corporation***
2788 San Tomas Expressway
Santa Clara, CA 95051
United States of America

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-2500006-01-CR**

Report version: 1

Project number: **NSCIB-2500006-01**

Author(s): **Andy Brown**

Date: 19 February 2026

Number of pages: **11**

Number of appendices: **0**

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, TrustCB 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 TrustCB 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 TrustCB 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, TrustCB 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.

Recognition of the Certificate

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 NVIDIA DRIVE OS Virtualization Software v6.0.9.3.1. The developer of the NVIDIA DRIVE OS Virtualization Software v6.0.9.3.1 is NVIDIA Corporation located in Santa Clara, CA, 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 (Target of Evaluation) is the NVIDIA DRIVE® virtualization solution. It is a type 1 hypervisor developed by NVIDIA Corporation, intended for automotive applications with extra safety requirements.

The TOE has the following features:

- Spatial isolation between VMs and between VMs and TOE components.
- Identification of TOE components and VMs.
- Controllable access to the services and data provided by TOE.
- Controllable access to the hardware resources provided by NVIDIA DRIVE AGX Orin™ SoC.
- Controllable access to the communication channels provided by TOE.
- Secure access to the functionalities implemented in CCPLEX Secure World.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 19 February 2026 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 NVIDIA DRIVE OS Virtualization Software v6.0.9.3.1, 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 NVIDIA DRIVE OS Virtualization Software v6.0.9.3.1 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 ALC_FLR.1 (Basic flaw remediation).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CEM:2022 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 *[CC]*.

TrustCB B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates. 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 NVIDIA DRIVE OS Virtualization Software v6.0.9.3.1 from NVIDIA Corporation located in Santa Clara, CA, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	kernel.bin (Binary image of Hypervisor Kernel)	6.0.9.3.1
	Sidekick (Binary image of VM Sidekick)	6.0.9.3.1
	pct.bin (Platform Configuration Table binary)	6.0.9.3.1
	Sysmgr (Binary image of System Manager)	6.0.9.3.1

To ensure secure usage a set of guidance documents is provided, together with the NVIDIA DRIVE OS Virtualization Software v6.0.9.3.1. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE implements a set of functionalities with the common goal – run Virtual Machines controlled by guest operating systems in an isolated virtualized environment and provide these Virtual Machines with the communication channels and services supported by the TOE in a secure way.

The TOE provides the following security features:

- Spatial isolation between VMs and between VMs and TOE components.
- Identification of TOE components and VMs.
- Controllable access to the services and data provided by TOE.
- Controllable access to the hardware resources provided by NVIDIA DRIVE AGX Orin™ SoC.
- Controllable access to the communication channels provided by TOE.
- Secure access to the functionalities implemented in CCPLEX Secure World.

The TOE is built upon a proprietary microkernel (Hypervisor Kernel) and includes additional entities running outside the microkernel that support functioning of Virtual Machines.

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]*.

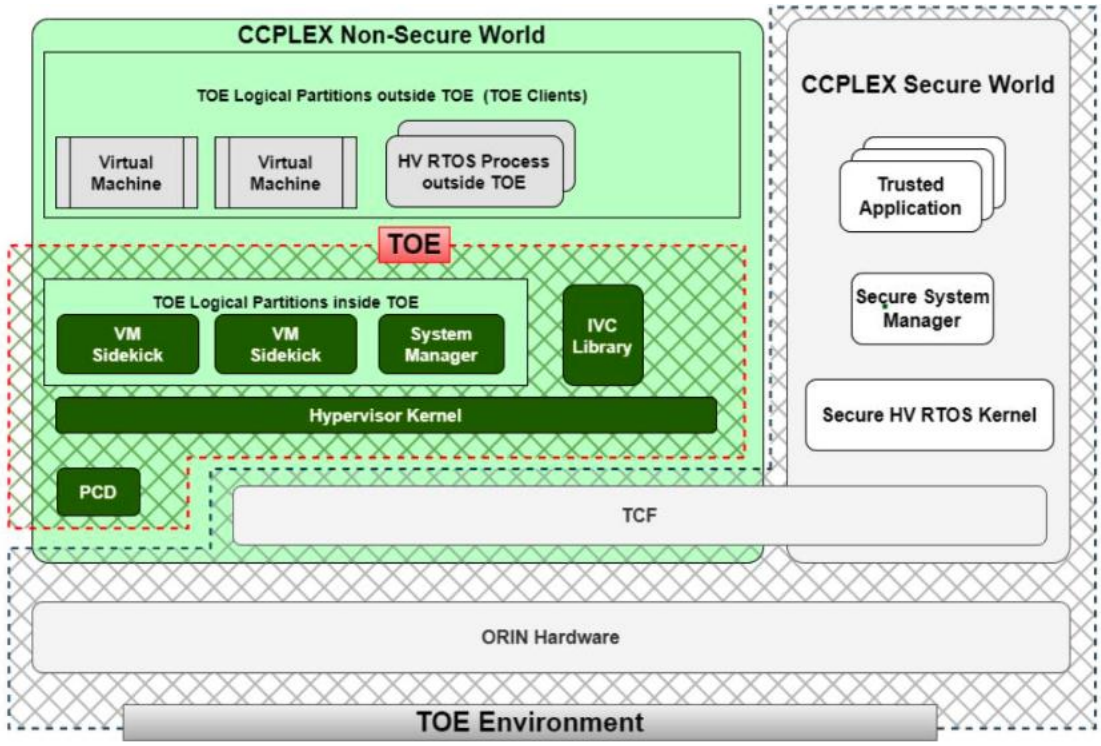
2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product. Retain this sentence only if there are no environmental assumptions and OSPs that counter threats to the TOE.

2.4 Architectural Information

The TOE (Target of Evaluation) is the NVIDIA DRIVE® virtualization solution. It is a type 1 hypervisor developed by NVIDIA Corporation, intended for automotive applications with extra safety requirements.

The logical architecture, originating from the Security Target *[ST]* of the TOE can be depicted as follows:



The TOE has the following security features:

- Spatial isolation between VMs and between VMs and TOE components.
- Identification of TOE components and VMs.
- Controllable access to the services and data provided by TOE.
- Controllable access to the hardware resources provided by NVIDIA DRIVE AGX Orin™ SoC.
- Controllable access to the communication channels provided by TOE.
- Secure access to the functionalities implemented in CCPLEX Secure World.

The TOE is built upon a proprietary microkernel (Hypervisor Kernel) and includes additional entities running outside the microkernel that support functioning of Virtual Machines. The TOE provides the following security features:

- Spatial isolation between VMs and between VMs and TOE components.
- Identification of TOE components and VMs.
- Controllable access to the services and data provided by TOE.
- Controllable access to the hardware resources provided by NVIDIA DRIVE AGX Orin™ SoC.
- Controllable access to the communication channels provided by TOE.
- Secure access to the functionalities implemented in CCPLEX Secure World.

The TOE is built upon a proprietary microkernel (Hypervisor Kernel) and includes additional entities running outside the microkernel that support functioning of Virtual Machines.

2.5 Documentation

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

Identifier	Version
NVIDIA DRIVE OS Virtualization Software AGD	1.1
NVIDIA DRIVE OS 6.0 QNX Cybersecurity Manual	1.2.1 DRIVE OS 6.0.9.3.1

NVIDIA DRIVE OS 6.X SEOOC SPECIFICATION	1.4 DRIVE OS 6.0.9.3.1
NVIDIA DRIVE OS 6.0 Safety Manual	1.2 DRIVE OS 6.0.9.3
NVIDIA DRIVE OS 6.0 QNX PDK Developer Guide	DRIVE OS 6.0.9.3.1 14/02/2025
NVIDIA DRIVE OS 6.0 QNX Installation Guide	DRIVE OS 6.0.9.3.1 02/03/2025
Interface Control Document of Virtualization System	DRIVE OS 6.0.9.3.1 08/10/2024
DRIVE OS SEooC SWADS	DRIVE OS 6.0.9.3.1 23/03/2025
Software Project Cybersecurity Plan for Virtualization System	DRIVE OS 6.0.9.3.1 12/11/2024

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

The evaluator repeated the complete test plan from the developer and also performed a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The evaluator defined independent tests to perform additional verifications to check the correct activation and behaviour of TOE's countermeasures under emulator conditions.

The penetration test plan included the distribution of the different test categories (following Common Weakness Enumeration system) as:

- CWE 20 Improper input handling (1 week)
- CWE 912 Hidden Functionality (1 week)
- CWE 345 Insufficient Verification of Data Authenticity (1 week)

The total test effort expended by the evaluators was 3 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The TOE was tested in the configuration: NVIDIA DRIVE OS Virtualization System v6.0.9.3.1.

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.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number NVIDIA DRIVE OS Virtualization Software v6.0.9.3.1.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the NVIDIA DRIVE OS Virtualization Software v6.0.9.3.1, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

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

3 Security Target

The NVIDIA DRIVE OS Virtualization Software Security Target, Version 2.7, 01 December 2025 *[ST]* is included here by reference.

4 Definitions

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

CA	Common Application
CCRA	Common Criteria Recognition Arrangement
CWE	Common Weakness Enumeration
HV	Hypervisor
IT	Information Technology
ITSEF	IT Security Evaluation Facility
IVC	Inter-VM Communication
MRA	Mutual Recognition Agreement
NSCIB	Netherlands Scheme for Certification in the area of IT Security
SMC	Secure Monitor Call
SoC	System on Chip
SOG-IS	Senior Official's Group Information Systems Security
TEE	Trusted Execution Environment
TOE	Target of Evaluation
VM	Virtual Machine

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 1 to 5, CC:2022 Revision 1, November 2022
[CCMB-2024-002]	Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[ETR]	Evaluation Technical Report NVIDIA DRIVE OS Virtualization Software v6.0.9.3.1 – EAL4+, 25-RPT-968, Version 4.0, 18 February 2026
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022
[ST]	NVIDIA DRIVE OS Virtualization Software Security Target, Version 2.7, 01 December 2025
[STAR-RNO]	Site Technical Audit Report - NVIDIA Reno DC6, 26-RPT-239, Version 1.0, 17 February 2026
[STAR-DC2]	Site Technical Audit Report - NVIDIA Santa Clara DC2, 26-RPT-240, Version 1.0, 17 February 2026
[STAR-HQ]	Site Technical Audit Report - NVIDIA Santa Clara HQ, 26-RPT-241, Version 1.0, 17 February 2026

(This is the end of this report.)