Version 2022-01

Certification Report

Huawei GaussDB(openGauss) Database Management System (DBMS) V500R001C20SPC100+V500R001C20HP1015

Sponsor and developer:	***Huawei Technologies Co., Ltd.*** **Huawei Industrial Base Bantian** **Longgang, Shenzhen 518129** **People's Republic of China**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0392006-CR**
Report version:	**1**
Project number:	**0392006**
Author(s):	**Andy Brown**
Date:	**31 August 2022**
Number of pages:	**11**
Number of appendices:	**0**

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Huawei GaussDB(openGauss) Database Management System (DBMS) V500R001C20SPC100+V500R001C20HP1015. The developer of the Huawei GaussDB(openGauss) Database Management System (DBMS) V500R001C20SPC100+V500R001C20HP1015 is Huawei Technologies Co., Ltd. located in Shenzhen, China 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 Database Management System (DBMS). It provides a relational database engine providing mechanisms for user access control, identification and authentication, data protection, and security audit. It mainly focuses on online transaction processing scenarios with large data volumes and high concurrency.

This TOE is a software-only TOE.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 31 August 2022 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 Huawei GaussDB(openGauss) Database Management System (DBMS) V500R001C20SPC100+V500R001C20HP1015, 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 Huawei GaussDB(openGauss) Database Management System (DBMS) V500R001C20SPC100+V500R001C20HP1015 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+ALC_FLR.2 assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Huawei GaussDB(openGauss) Database Management System (DBMS) V500R001C20SPC100+V500R001C20HP1015 from Huawei Technologies Co., Ltd. located in Shenzhen, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Huawei GaussDB(openGauss) Database Management System (DBMS)	V500R001C20SPC100 + V500R001C20HP1015

To ensure secure usage a set of guidance documents is provided, together with the Huawei GaussDB(openGauss) Database Management System (DBMS) V500R001C20SPC100+V500R001C20HP1015. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

To counter the security threats listed in the [ST], the TOE provides the following security features:

- **Security Audit.** Audit entries are generated for security related events. Moreover, the TOE supports selecting the set of events to be audited based on a set of attributes.
- **User Data Protection.** The TOE provides a discretionary access control policy (RBAC) to provide access control. It further controls that only authorized administrators are able to manage the TOE.
- **Identification and Authentication.** Identification and identity authentication are performed before users are allowed to access database objects.
- **Security Management.** The security functions associated with audit, access control, and user accounts are provided by the SQL command line interface and the parameter configuration tool on the server.
- **Protection of the TSF.** The consistency of replicated TSF data is protected by ensuring the consistency of the replicated TSF data upon reconnection before processing any requests.
- **TOE Access.** The Session Handling mechanism limits the possibilities of users to establish sessions with the TOE and maintains a separate execution context for every operation.

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 5.2.1 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.

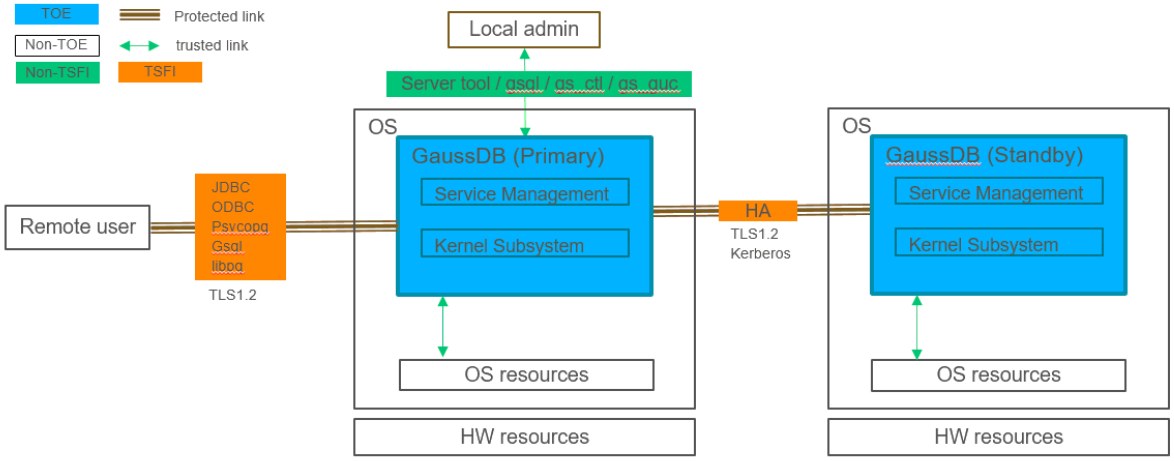
2.4 Architectural Information

The TOE is a DBMS. It provides a relational database engine providing mechanisms for user access control, identification and authentication, data protection, and security audit. It mainly focuses on online transaction processing scenarios with large data volumes and high concurrency.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

The TOE is software-only.

The logical architecture can be depicted as follows:



The TOE can restrict the access of authorized users to the TOE, implement discretionary access control on objects controlled by the DBMS based on users or roles, and can clarify users' responsibilities by their behaviour.

TOE security functions include security audit, user data protection, identity identification and authentication, security management, data backup and restoration, ensuring database security.

2.5 Documentation

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

Identifier	Version
HUAWEI GaussDB Kernel V500R001C20SPC100+ V500R001C20HP1015 AGD_PRE	0.12
HUAWEI GaussDB Kernel V500R001C20SPC100+ 0.12 V500R001C20HP1015 AGD_OPE	0.11
GaussDB Kernel V500R001C20SPC100+V500R001C20HP1015 Product Documentation	0.4
GaussDB Kernel V500R001C20SPC100+V500R001C20HP1015 Communication Matrix	03

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 developer undertook functional testing covering all TSFI's and subsystems focussing on the gsql interface and security functionalities. A list of tests was executed by an automatic test framework tool created by the developer. A preparation procedure was provided in the evaluation evidence which also specified the list of automated and non-automated test cases. 75% of the test case were automated and 25% manual.

The independent evaluator repeat testing focused on doing the maximum number of developer's test cases which covered a significant amount of the TSF, namely:

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

- Security Audit.
- User Data Protection.
- User Identification and Authentication.
- Security Management.
- Protection of the TSF.
- TOE Access.

In addition to the automated tests, a sample of manual tests was chosen to ensure that the repeated developer test plan covered all TSFIs and modules of the TOE Design. The evaluator ensured that the automatic tests covered all TSFIs and modules of the TOE not covered by the manual independent tests.

The evaluator defined further tests to cover more scenarios and gain extra assurance from existing test cases.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- Source Code review.
- Vulnerabilities resulting from a search through the ST, the functional specification, the TOE design, the security architecture description and the guidance documentation.
- Public vulnerabilities stemming from previous products, dependencies and the public domain.

From this analysis, penetration tests were created. The total test effort expended by the evaluators was 9 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

The TOE was tested in the following configurations:

- Single node configuration running on x86_64 server.
- Multi-node (HA) configuration running on 3 instances of x86_64 servers consisting of one
- primary and two standby nodes.
- In addition to the information about the operating system in *[ST]*, Python 2.7 used the library psycopg2 v2.8.6.

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.

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 a Site Technical Audit Reuse report.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei GaussDB(openGauss) Database Management System (DBMS) V500R001C20SPC100+V500R001C20HP1015.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 Report(s) for the site(s) *[STAR-BDC]* and *[STAR-HDC]* [2].

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

Based on the above evaluation results the evaluation lab concluded the Huawei GaussDB(openGauss) Database Management System (DBMS) V500R001C20SPC100+V500R001C20HP1015, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.2**. 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]*.

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 TOE user guidance. 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.

[2] 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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

3 Security Target

The Huawei GaussDB Kernel V500R001C20SPC100+V500R001C20HP1015 Security Target, 0.18, 07 June 2022 *[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:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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
[ETR]	Evaluation Technical Report Huawei GaussDB (openGauss) V5 – EAL4+, 21-RPT-470, 5.0, 25 August 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[PP]	Protection Profile for Database Management Systems (Base Package), BSI-CC-PP-0088-V2, Version 2.12, 23 March 2017.
[ST]	Huawei GaussDB Kernel V500R001C20SPC100+V500R001C20HP1015 Security Target, 0.18, 07 June 2022
[STAR-BDC]	Site Technical Audit Report Huawei Beijing Development Site, 21-RPT-1061, v3.0, 07 June 2022.
[STAR-HDC]	Site Technical Audit Report Huawei Beijing Huitian Data Center site, 21-RPT-1062, v3.0, 07 June 2022.

(This is the end of this report.)

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.