SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-112 CR Certification Report

Issue 1.0 10 October 2018

Expiry date 10 October 2023

Rubrik Cloud Data Management v 4.1.2

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE ST 009E VERSION 2.5 15.05.2018

SERTIT, P.O. Box 814, N-1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party’s claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The recognition under CCRA is limited to cPP related assurance packages or components up to EAL 2 with ALC_FLR CC part 3 components.

Contents

1 Certification Statement 5

2 Abbreviations 6

3 References 7

4 Executive Summary 8
4.1 Introduction 8
4.2 Evaluated Product 8
4.3 TOE scope 8
4.4 Protection Profile Conformance 8
4.5 Assurance Level 9
4.6 Security Policy 9
4.7 Security Claims 9
4.8 Threats Countered 9
4.9 Threats Countered by the TOE's environment 9
4.10 Threats and Attacks not Countered 9
4.11 Environmental Assumptions and Dependencies 10
4.12 Evaluation Conduct 10
4.13 General Points 10

5 Evaluation Findings 12
5.1 Introduction 12
5.2 Delivery 13
5.3 Installation and Guidance Documentation 13
5.4 Misuse 13
5.5 Vulnerability Analysis 13
5.6 Developer's Tests 13
5.7 Evaluators' Tests 14

6 Evaluation Outcome 15
6.1 Certification Result 15
6.2 Security Target 15
6.3 Recommendations 15

Annex A: Evaluated Configuration 16
TOE Identification 16
TOE Documentation 16
TOE Configuration 16

1 Certification Statement

Rubrik Cloud Data Management is a software platform that distributes data, metadata and task management across the cluster in order to deliver predictive scalability and eliminate performance bottlenecks.

Rubrik Cloud Data Management version 4.1.2 has been evaluated under the terms of the Norwegian Certification Authority for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality in the specified environment when running on the platforms specified in Annex A.

Certification team	Arne Høye Rage, SERTIT Kjartan Kvassnes, SERTIT
Date approved	10 October 2018
Expiry date	10 October 2023

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation(ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
cPP	collaborative Protection Profile
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
POC	Point of Contact
PP	Protection Profile
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SOGIS MRA	SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] SERTIT (2018), *The Norwegian Certification Scheme*, SD001E, Version 10.4, SERTIT, 20 February 2018.

[2] CCRA (2017), *Common Critera for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2017-04-001, Version 3.1 R5, CCRA, April 2017.

[3] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2017-04-002, Version 3.1 R5, CCRA, April 2017.

[4] CCRA (2017), *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB- 2017-04-003, Version 3.1 R5, CCRA, April 2017.

[5] CCRA (2017), *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2017-04-004, Version 3.1 R5, CCRA, April 2017.

[6] CCRA (2006), *ST sanitising for publication*, 2006-04-004, CCRA, April 2006.

[7] SOGIS Management Committee (2010), *Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, Version 3.0, SOGIS MC, January 8th 2010.

[8] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, July 2nd 2014.

[9] Rubrik Cloud Data Management Security Target Version 1.2. 2018-09-10.

[10] ETR for the evaluation project SERTIT-112 Common Criteria EAL2 Augmented with ALC_FLR.1 Evaluation of Rubrik Cloud Data Management version 1.1. 2018-09-10

Guidance documents are listed in Annex A.

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Rubrik Cloud Data Management version 4.1.2 to the Sponsor, Rubrik, Inc., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the ST [9] which specifies the functional, environmental and assurance evaluation components.

4.2 Evaluated Product

The version of the product evaluated was Rubrik Cloud Data Management and version 4.1.2.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Rubrik, Inc.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

TOE is purely software and can be installed on several physical devices if the following non-TOE requirements are valid.

TOE requires the following non-TOE hardware:

- A VMware ESXi server used for running Rubrik Edge, which is a commodity computer (that is centrally managed by the Rubrik cluster).

TOE requires the following non-TOE software:

- Rubrik Edge, which is a virtualized software-only version of the Rubrik Cloud Data management product.

TOE requires the following non-TOE software:

- VMware ESXi, which is the host environment for a Rubrik Edge virtual machine.

TOE requires the following non-TOE software:

- Rubrik Backup Connector, which is installed on each backup source, is required to do a backup of the physical infrastructure.

4.4 Protection Profile Conformance

The ST [9] did not claim conformance to any protection profile/cPP.

4.5 Assurance Level

The ST [9] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL 2 augmented with ALC_FLR.1 was used. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.

P.CRYPTOGRAPHIC The TOE shall provide cryptographic functions for its own use, including encryption/decryption operations.

4.7 Security Claims

The ST[9] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional components and security functions to elaborate the objectives. Most of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

The ST[9] chapter 5.1 specifies one extended SFR.

4.8 Threats Countered

TT.ADMIN_ERROR The TOE may be incorrectly configured that may result in the TOE's acquisition of ineffective security mechanisms.

TT.ADMIN_EXPLOIT A person/company may gain access to an administrator account.

TT.CRYPTO_COMPROMISE An attacker may compromise cryptographic keys and the data protected by the cryptographic mechanisms.

TT.HACK_ACCESS A person/company gets undetected system access to the TOE due to missing, weak and/or incorrectly implemented access control, causing potential violations of integrity, confidentiality or availability.

TT.MALFUNCTION The TOE may malfunction which may compromise information and data processing**.**

4.9 Threats Countered by the TOE's environment

TE.EAVESDROPPING Eavesdropping of the communication between Rubrik nodes. This includes man-in-the-middle, side-channel, or other redirection attacks.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

A.TRUSTED_ADMIN The administrators of the TOE shall not have any malicious intention, shall receive proper training on the TOE management, and shall follow the administrator guidelines.

4.12 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[1]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of both the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, CCRA[8], and the Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, SOGIS MRA[7] and the evaluation was conducted in accordance with the terms of these Arrangements.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its ST[9], which prospective consumers are advised to read. To ensure that the ST[9] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[5].

SERTIT monitored the evaluation in accordance with SD001E[1] which was carried out by the Advanced Data Security Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final ETR[10] to SERTIT in 10 September 2018. SERTIT then produced this Certification Report.

4.13 General Points

The evaluation addressed the security functionality claimed in the ST[9] with reference to the assumed operating environment specified by the ST[9]. The evaluated configuration is specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this

Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 2 assurance package augmented with ALC_FLR.1.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.1	Basic flaw remediation
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

5.1 Introduction

The evaluation addressed the requirements specified in the ST[9]. The results of this work were reported in the ETR[10] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the User Guidance documents provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

The guidance documents are listed in Annex A.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process. The evaluators have examined sources of information publicly available to identify potential vulnerabilities in the TOE and also conducted a search of ST, guidance documentation, functional specification, TOE design and security architecture description evidence to identify possible potential vulnerabilities in the TOE.

Based on this the evaluators performed a set of penetration tests and the verdict is that the TOE is resistant against attackers possessing Basic attack potential.

5.6 Developer's Tests

The evaluators have examined the developers test coverage evidence and determined that the correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification is accurate.

The evaluators have examined the test plan and determined that it describes the scenarios for performing each test, including any ordering dependencies on results of other tests.

The developer's tests concentrate on critical functionality of the TOE. The test results were integrated into the description of the tests, or provided separately. All results were of passing grade

The evaluators conclusion is that the tests satisfy the requirements of EAL2.

5.7 Evaluators' Tests

The evaluators have employed a combination of a random sampling method and a method based on the intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible. The evaluators took into consideration the potential security impact of the tests, as well as the number of subsystems that contribute to successful completion of the tests.

For independent testing the evaluators have employed a method based on the intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible. The evaluators took into consideration the potential security impact of the tests, as well as the number of subsystems that contribute to successful completion of the tests.

The independent tests concentrated on critical functionality of the TOE. All results were of passing grade.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[10], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Rubrik Cloud Data Management version 4.1.2 meet the specified Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 extended functionality in the specified environment, when running on platforms specified in Annex A.

6.2 Security Target

The developer did not provide a Security Target Lite and acceped to publish the complete Security Target [9] used for the evaluation.

6.3 Recommendations

Prospective consumers of Rubrik Cloud Data Management version 4.1.2 should understand the specific scope of the certification by reading this report in conjunction with the ST [9]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST [9].

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE is Rubrik Cloud Data Management with Rubrik Version 4.1.2.

TOE is purely software and can be installed on several physical devices if the non-TOE requirements below are valid

TOE requires the following non-TOE hardware:

- A VMware ESXi server used for running Rubrik Edge, which is a commodity computer (that is centrally managed by the Rubrik cluster).

TOE requires the following non-TOE software:

- Rubrik Edge, which is a virtualized software-only version of the Rubrik Cloud Data management product
- VMware ESXi, which is the host environment for a Rubrik Edge virtual machine.
- Rubrik Backup Connector, which is installed on each backup source, is required to do a backup of the physical infrastructure.

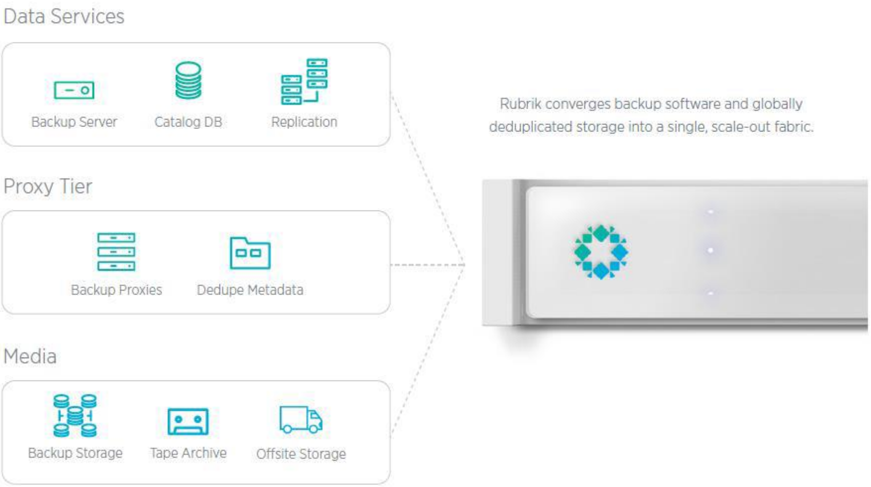
TOE Documentation

The supporting guidance documents evaluated were:

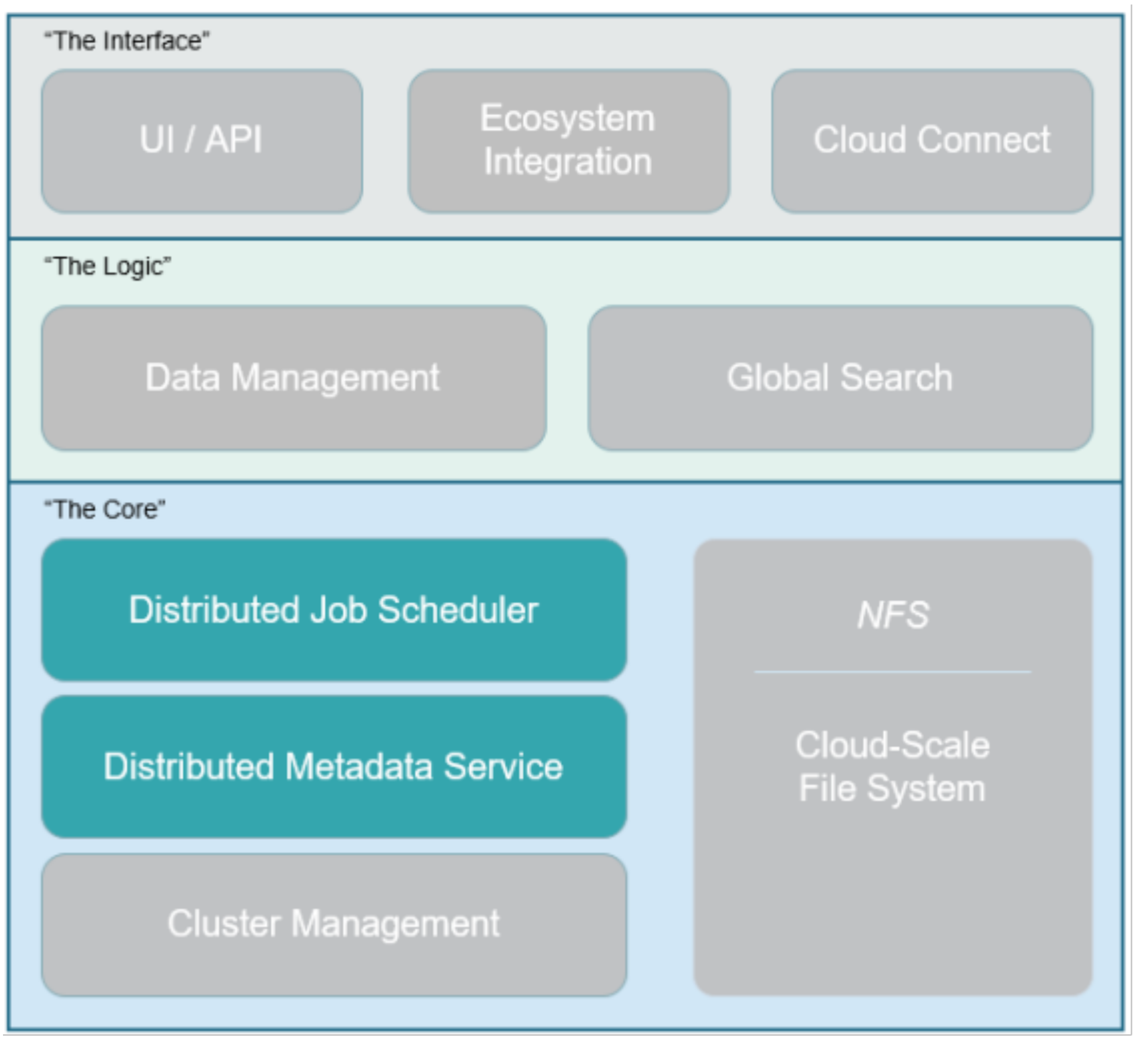
[a] Rubrik Cloud Data Management Security Target 2018-09-10 Version 1.2
[b] Rubrik User Guide, Version 4.1
[c] Rubrik CLI Reference Guide, Version 4.1
[d] Rubrik Guidance Documentation, v. 1.3
[e] Rubrik REST API for Rubrik 4.1, Version 1.0

TOE Configuration

The following configuration was used for testing:



Single Converged, Scale-out Fabric



Rubrick Stack

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunctionwith the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Certificate

Certificate Identifier: SERTIT-112 C

Product Name: Rubrik Cloud Data Management

Version and Release Numbers: 4.1.2

Type of Product: Other Devices and Systems

Product Manufacturer: Rubrik, Inc.

Assurance Type: EAL 2 augmented with ALC_FLR.1

Evaluation Criteria: Common Criteria Version 3.1 R5

Name of IT Security Evaluation Facility: Advanced Data Security

Name of Validation Body and Certification Authority: SERTIT

Certification Report Identifier: SERTIT-112 CR, issue 1.0, 10 October 2018

Certificate Issued Date: 10 October 2018 Certificate Expiry Date: 10 October 2023

Arne H. Rage

Arne Høye Rage
Certifier

Kjartan Kvassnes
Quality Assurance

Jørn Arnesen
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

CC Recognition Arrangement
for cPPs or components up to
EAL 2 and ALC_FLR