KECS-CR-23-31

OTACToken V1.0

Certification Report

Certification No.: KECS-CISS-1237-2023

2023. 5. 3.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2023.05.03.	-	Certification report for OTACToken V1.0 - First documentation

This document is the certification report for OTACToken V1.0 of SSenStone Inc.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KoSyAs)

Table of Contents

1. Executive Summary 5
2. Identification 8
3. Security Policy 9
4. Assumptions and Clarification of Scope 9
5. Architectural Information 9
1. Physical Scope of TOE 9
2. Logical Scope of TOE 10
6. Documentation 12
7. TOE Testing 13
8. Evaluated Configuration 13
9. Results of the Evaluation 14
1. Security Target Evaluation (ASE) 14
2. Development Evaluation (ADV) 15
3. Guidance Documents Evaluation (AGD) 15
4. Life Cycle Support Evaluation (ALC) 15
5. Test Evaluation (ATE) 15
6. Vulnerability Assessment (AVA) 16
7. Evaluation Result Summary 16
10. Recommendations 17
11. Security Target 18
12. Acronyms and Glossary 19
13. Bibliography 20

1. Executive Summary

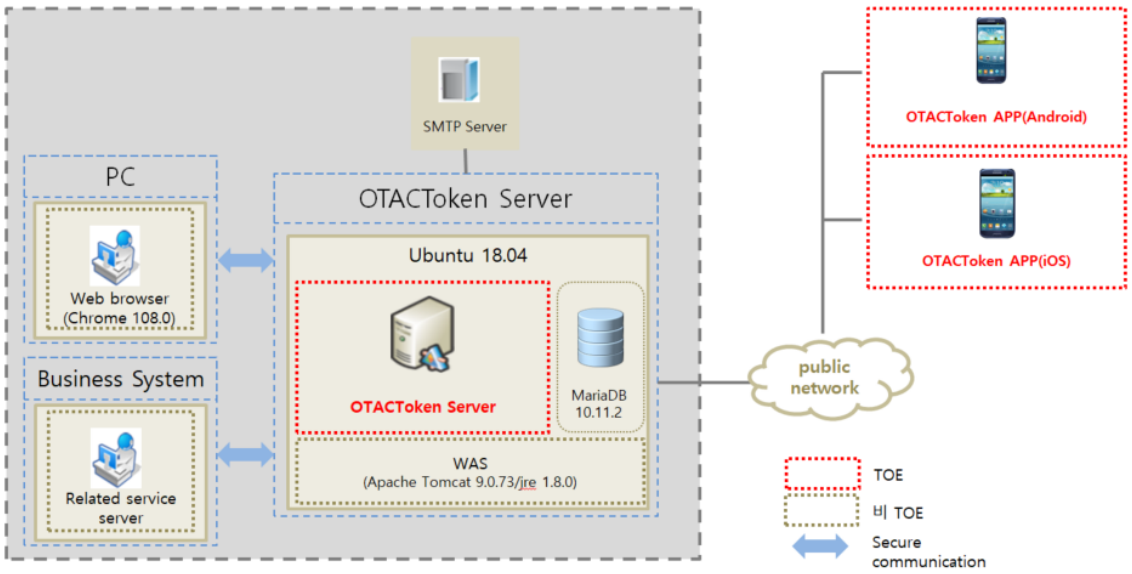
This report describes the evaluation result drawn by the evaluation facility on the results of the OTACToken V1.0 developed by SSenStone Inc. with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter)[1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (“TOE” hereinafter) is simple authentication solution that allows users to access the work systems through mobile devices using an OTAC authentication code for various work services.

After being initialized, the TOE periodically performs integrity checks, performs identification and authentication, and authentication failure response capabilities while limiting duplicate logins for the same administrator. If the repository protection limit set by the authorized administrator to protect the audit data repository is exceeded, a warning email will be sent to the administrator, and TOE also provides TSF protection functions such as security audit functions for recording and managing audit data, protection function of data saved in the repository controlled by the TSF and TSF self-test, etc. for major events during the operation of security functions and management functions. In addition, the TOE provides access and integrity functions for managing the authorized administrator's access sessions. The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on April 07, 2023.

The ST has no conformance claim to the Protection Profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1. Therefore, the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore, the ST and the resulting TOE is CC Part 2 extended.

[Figure-1] shows the operational environment where the TOE is operated. TOE operating environment consists of the OTACToken Server and the OTACToken APP (Android) / OTACToken APP (iOS). The security management of TOE is performed through a web browser (Chrome) that supports HTTPS (Hypertext Transfer Protocol over Secure Socket Layer). OTACToken APP (Android) / OTACToken APP (iOS) performs the function of generating a one-time authentication code for user authentication of the work system when it is executed.



[Figure 1] TOE Operational Environment

The requirements for hardware, software and operating system to install the OTACToken Server are shown in [Table 1].

Classification		Requirement
HW	CPU	Intel(R) Core(TM) i5-6400 CPU @ 2.70GHz 4core or higher
	Memory	8 GB or higher
	HDD	Space required for TOE installation is 150 MB or higher
	NIC	10/100/1000 Mbps * 1 EA or higher
SW	OS	Ubuntu 18.04 (64bit) (kernel 5.4.0-139)
	DBMS	MariaDB 10.11.2
	WAS	Apache Tomcat 9.0.73
	JRE	jre 1.8.0_362

[Table 1] OTACToken Server Hardware and Software specifications

The requirements for hardware, software and operating system to install the OTACToken APP(Android) are shown in [Table 2].

Product	Model	OS	
		Version	Kernel
SAMSUNG Galaxy S22	SM-S901N	13	5.10.81

[Table 2] OTACToken APP(Android) Hardware and Software specifications

The requirements for hardware, software and operating system to install the OTACToken APP(iOS) are shown in [Table 3].

Product	Model	OS	
		Version	Kernel
iPhone 13	A2633	15.4.1	-

[Table 3] OTACToken APP(iOS) Hardware and Software specifications

The requirements for software of Managed PC are shown in [Table 4]

Classification	Requirement
SW	Chrome 108.0

[Table 4] Managed PC Software specifications

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE reference is identified as follows.

TOE		OTACToken V1.0
TOE detailed version		V1.0.02.02.02
TOE Components	OTACToken Server	OTACToken Server V1.0.02
	OTACToken APP(Android)	OTACToken App(Android) V1.0.02
	OTACToken APP(iOS)	OTACToken App(iOS) V1.0.02
Guidance		OTACToken V1.0 Administrator's Manual V1.4
		OTACToken V1.0 User Manual V1.4
		OTACToken V1.0 Installation Guide V1.4

[Table 5] TOE identification

[Table 6] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea IT Security Evaluation and Certification Guidelines (October 31, 2022) Korea IT Security Evaluation and Certification Regulation (May 17, 2021)
TOE	OTACToken V1.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April 2017
EAL	EAL1+ (ATE_FUN.1)
Protection Profile	ST does not claim conformance to PP
Developer	SSenStone Inc.
Sponsor	SSenStone Inc.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	April 07, 2023

[Table 6] Additional identification information

3. Security Policy

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted path

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) [3]

4. Assumptions and Clarification of Scope

There are no Assumptions in the Security Problem Definition in the ST. The scope of this evaluation is limited to the functionality and assurance covered in the Security Target. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process. (for the detailed information of TOE version and TOE Components version refer to the [Table 4])

5. Architectural Information

1. Physical Scope of TOE

The physical scope that makes up the TOE is the OTACToken Server, OTACToken App(Android), OTACToken APP(iOS) and guidelines (administrator manual, user manual, Installation Guide) as shown in the below [Figure 3]. Hardware, operating system, DBMS, WAS, JDK, Wrapper which are operating environments of the TOE are excluded from the physical scope of the TOE. Hardware, operating system, DBMS which are operating environments of the TOE are excluded from the physical scope of the TOE.

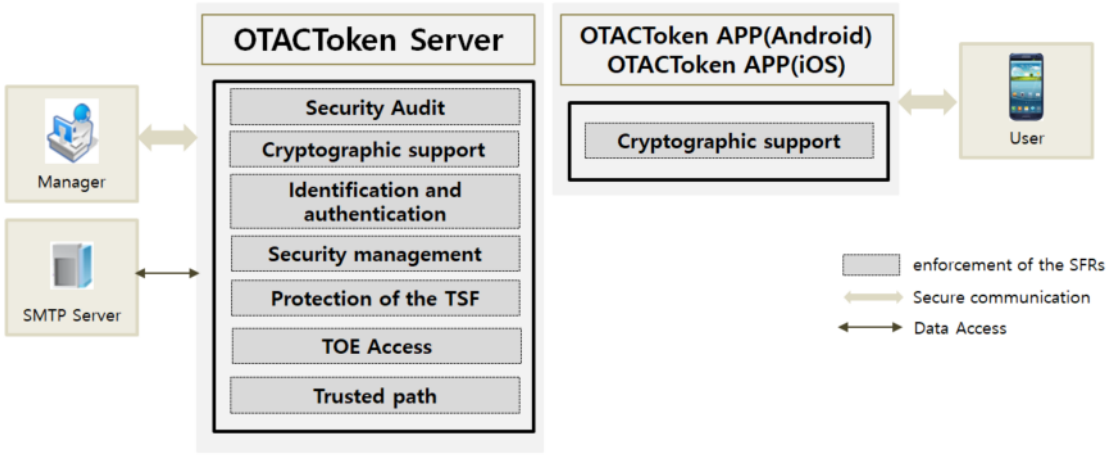
Classification		Identification	Type
TOE component	OTACToken Server	OTACToken Server V1.0.02 **- OTACToken Server V1.0.02.tar**	Software (Distributed as a CD)
	OTACToken App(Android)	OTACToken App(Android) V1.0.02 - OTACToken App(Android) V1.0.02.apk	

	OTACToken App(iOS)	OTACToken App(iOS) V1.0.02 - OTACToken App(iOS) V1.0.02.ipa	
Guidance		OTACToken V1.0 Administrator's Manual V1.4 **- OTACToken V1.0 Administrator's Manual V1.4.pdf**	PDF (Distributed as a CD)
		OTACToken V1.0 User Manual V1.4 **- OTACToken V1.0 User Manual V1.4.pdf**	
		OTACToken V1.0 Installation Guide V1.4 **- OTACToken V1.0 Installation Guide V1.4.pdf**	

[Table 7] Physical scope of TOE

2. Logical Scope of TOE

The logical scope of the TOE is as in [Figure 3] below.



[Figure 2] TOE Logical scope

▣ Security Audit

OTACToken Server generates audit data for TSF data management and security management provided through a web browser.

Audit data will be generated for security management and configuration, information changes, identification and authentication of TSF data, integrity checks, starting and ending

of audit functions, and audit data for security violations.

The generated audit data includes the log creation time, the subject's identity, the event result(success or failure), the items related to the event type, and audit data that is additionally created.

The audit data will be stored in a DBMS and be provided to authorized administrators in an appropriate format through a web browser.

▣ Cryptographic support

OTACToken Server generates symmetric keys through a random bit generator, encrypts the generated OTAC information using the symmetric key, and then transmits the encrypted data to the work system.

- Random Number Generator : SP 800-90A HMAC DRBG(Deterministic Random Bit Generator)
- Symmetric Key Algorithm : AES 128 Bit

OTACToken APP(Android)/OTACToken APP(iOS) reads and decrypts the OTAC information provided by the QR code, and generates a new symmetric key to encrypt the OTAC information and store it in the APP storage space.

- Public Key Algorithm : RSA 2048 Bit
- Symmetric Key Algorithm : AES 128 Bit

OTACToken APP(Android)/OTACToken APP(iOS) also provides the OTAC data by decrypting the stored OTAC information using the symmetric key when a request for OTAC code generation is made for user authentication.

▣ Identification and authentication

When attempting identification and authentication, the administrator will be identified by ID and the administration authentication will be performed before any action. The password for authentication will be displayed as '•' and only information on the cause of authentication failure is provided to prevent password exposure.

The administrator's password must be created according to password rules, and if identification and authentication are successful, the administrator maintains security management authority. When attempting authentication through a web browser, if the authentication attempt failure count (5 times) is exceeded, the account will be locked for 5 minutes.

▣ Security Management

OTACToken Server sets security policies for each service (work system) and manages administrators and registered users.

▣ Protection of the TSF

OTACToken Server protects the TSF data transmitted between the TOE and web browsers from exposure or modification and also protects the stored information from unauthorized exposure or modification.

OTACToken Server also periodically performs integrity checks and self-tests after startup.

▣ TOE access

The administrator automatically terminates the session if it is not used for a period of inactivity and requires reauthentication for reuse.

In addition, for administrator sessions for security management, the maximum number of session connections is limited to one to prevent duplicate logins.

▣ Trusted path

OTACToken Server provides a communication path that protects communication data from being altered or exposed by remote users through a trusted path.

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identification	Date
OTACToken V1.0 Administrator's Manual V1.4 - OTACToken V1.0 Administrator's Manual V1.4.pdf	April 24, 2023
OTACToken V1.0 User Manual V1.4 - OTACToken V1.0 User Manual V1.4.pdf	April 24, 2023
OTACToken V1.0 Installation Guide V1.4 - OTACToken V1.0 Installation Guide V1.4.pdf	April 24, 2023

[Table 8] Documentation

7. TOE Testing

The evaluator conducted independent testing listed in Independent Testing Report [4], based upon test cases devised by the evaluator. The evaluator took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no.: Identifier of each test case
- Test Purpose: Includes the security functions to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator set up the test configuration and testing environment consistent with the ST [3]. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover weakness analysis of privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing. The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the Penetration Testing Report [5].

8. Evaluated Configuration

The TOE is software consisting of the following components:

TOE: OTACToken V1.0 (V1.0.02.02.02)

- OTACToken Server V1.0.02
- OTACToken App(Android) V1.0.02
- OTACToken App(iOS) V1.0.02

The Administrator can identify the complete TOE reference after installation using the product’s Info check menu. And the guidance documents listed in this report chapter 7 were

evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility wrote the evaluation result in the ETR which references Single Evaluation Reports for each assurance requirement and Observation Reports. The evaluation result was based on the CC [1] and CEM [2]. The TOE was evaluated based on Common Criteria for Information Technology Security Evaluation. (EAL1+).

1. Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore, the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore, the verdict PASS is assigned to ASE_CCL.1.

The Security Objectives for the operational environment are clearly defined. Therefore, the verdict PASS is assigned to ASE_OBJ.1.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore, the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and they are internally consistent. Therefore, the verdict PASS is assigned to ASE_REQ.1.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore, the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict **PASS** is assigned to the assurance class ASE.

2. Development Evaluation (ADV)

The functional specifications specify a high-level description of the SFR-enforcing and SFR-supporting TSFIs, in terms of descriptions of their parameters. Therefore, the verdict PASS is assigned to ADV_FSP.1.

The verdict **PASS** is assigned to the assurance class ADV.

3. Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore, the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore, the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict **PASS** is assigned to the assurance class AGD.

4. Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore, the verdict PASS is assigned to ALC_CMC.1.

The configuration management document verifies that the configuration list includes the TOE and the evaluation evidence. Therefore, the verdict PASS is assigned to ALC_CMS.1.

Also, the evaluator confirmed that the correct version of the software is installed in device.

The verdict **PASS** is assigned to the assurance class ALC.

5. Test Evaluation (ATE)

The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation.

Therefore, the verdict PASS is assigned to ATE_IND.1. Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict **PASS** is assigned to the assurance class ATE.

6. Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore, the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don't allow attackers possessing basic attack potential to violate the SFRs.

The verdict **PASS** is assigned to the assurance class AVA.

7. Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ALC	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	PASS
	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	
ATE	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	PASS
	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 9] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The TOE must be installed and operated in a physically secure environment accessible only by authorized administrators and should not allow remote management from

outside.

- The administrator shall maintain a safe state such as application of the latest security patches, eliminating unnecessary service, change of the default password, etc., of the operating system and DBMS in the TOE operation.

- The administrator should periodically checks a spare space of audit data storage in case of the audit data loss, and carries out the audit data backup to prvent audit data loss.

11. Security Target

OTACToken V1.0 Security Target V1.7 [3] is included in this report for reference.

12. Acronyms and Glossary

(1) Acronyms

CC Common Criteria
CEM Common Methodology for Information Technology Security Evaluation
EAL Evaluation Assurance Level
ETR Evaluation Technical Report
OR Observation Report
SAR Security Assurance Requirement
SFR Security Functional Requirement
ST Security Target
TOE Target of Evaluation
TSF TOE Security Functionality
TSFI TSF Interface

(2) Glossary

Random bit generator
A device or algorithm that outputs a binary string that is statistically independent and is not biased. The RBG used for cryptographic application generally generates 0 and 1 bit string, and the string can be combined into a random bit block. The RBG is classified into the deterministic and non-deterministic type. The deterministic type RBG is composed of an algorithm that generates bit strings from the initial value called a “seed key,” and the non-deterministic type RBG produces output that depends on the unpredictable physical source.

Attack potential
Measure of the effort to be expended in attacking a TOE expressed as an attacker's expertise, resources and motivation.

Management access
The access to the TOE by using the HTTPS, SSH, TLS, etc to manage the TOE by administrator, remotely.

Symmetric cryptographic technique
Encryption scheme that uses the same secret key in mode of encryption and

decryption, also known as secret key cryptographic technique.

Decryption
The act that restoring the ciphertext into the plaintext using the decryption key.

Secret Key
The cryptographic key which is used in symmetric cryptographic algorithm and is associated with on or more entity, it is not allowed to release.

Identity
Representation uniquely identifying entities (e.g. user, process or disk) within the context of the TOE.

Encryption
The act that converting the plaintext into the ciphertext using the cryptographic key.

External Entity
any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.

Threat Agent
Unauthorized external entities that pose threats such as illegal access, alteration, or deletion of assets.

Authorized Administrator
Users who can execute functions according to Security Functional Requirements (SFRs)

Authentication Data
information used to verify the claimed identity of a user.

13. Bibliography

The evaluation facility has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-001 ~ CCMB-2017-04-003, April, 2017

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, CCMB-2017-04-004, April, 2017

[3] OTACToken V1.0 Security Target V1.7, April 24, 2023

[4] OTACToken V1.0 Independent Testing Report (ATE_IND.1) V2.00, April 25, 2023

[5] OTACToken V1.0 Penetration Testing Report (AVA_VAN.1) V2.00, April 25, 2023