Certification Report

EAL4+ (AVA_VAN.5) Evaluation of

SAYTEC SİBER SAVUNMA TEKNOLOJİLERİ A.Ş.
sayTRUST Secure Access System v0.6

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-99

TABLE OF CONTENTS

Document Information

Date of Issue	**28/10/2025**
Approval Date	**05/11/2025**
Certification Report Number	**21.0.03/25-005**
Developer	**SAYTEC SİBER SAVUNMA TEKNOLOJİLERİ A.Ş.**
Sponsor	**MİKROLİNK BİLİŞİM SAN. TİC. A.Ş.**
Evaluation Facility	**BEAM TEKNOLOJİ A.Ş.**
TOE/ PP Name*	**sayTRUST Secure Access System v0.6**
Pages	**22**

Prepared by ***Common Criteria Inspection Expert***	**Yavuz AVCI**
Reviewer (Approver)	**Mert LENGERLİOĞLU**

The experts whose names and signatures are shown as above prepared and reviewed this report.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	28/10/2025	All	First Release

DISCLAIMER

This certification report and the IT product/PP defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 5, using Common Methodology for IT Products Evaluation, version 3.1, revision 5. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria

document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by BEAM TEKNOLOJİ A.Ş., which is a commercial CCTL.

A Common Criteria Certificate given to a product means that such product meets the security requirements defined in its security target/PP document that has been approved by the CCCS. The Security Target document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for sayTRUST Secure Access System v0.6 whose evaluation was completed on November 21st 2024 and

whose evaluation technical report was drawn up by BEAM TEKNOLOJİ A.Ş. (as CCTL), and with the Security Target document with version no 3.6 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by the Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including *EAL2*. The current list of signatory nations and approved certification schemes can be found on:

https://www.commoncriteriaportal.org

1 - EXECUTIVE SUMMARY

Developer of the IT product: SAYTEC SİBER SAVUNMA TEKNOLOJİLERİ A.Ş.

Evaluation Sponsor of the IT product: MİKROLİNK BİLİŞİM SAN. TİC. A.Ş.

Evaluated IT product: sayTRUST Secure Access System

IT Product Version: 0.6

Name of IT Security Evaluation Facility: BEAM TEKNOLOJİ A.Ş.

Completion date of evaluation: 21/11/2024

Assurance Package: EAL 4+ (AVA_VAN.5)

1.1. Brief Description

sayTRUST Secure Access System v0.6 (hereinafter TOE) consists of software parts that take part in the implementation of the VPSC based SayTRUST® Access solution and allows users to provide a secure connection to private networks from public networks.

The software parts of the TOE on client-side and server-side are given below:

- ***On the client-side (sayTRUST Access Client)***
  - The client part of the TOE is "*sayTRUST Access Client Application*" and "*Crypto Libraries*" stored on the USB Stick.
- ***On the server-side (sayTRUST Access Server)***
  - The server part of TOE is the Linux based customized Operating System (*sayTRUST Access Server Operating System*) that can be used by directly installing on a dedicated sayTRUST Access Appliance or on an existing hardware or can be used as virtualized on a virtual machine.

1.2. Major Basic Security and Functional Attributes

Since the TOE consists of both the client part and server part, the description of the following security features is emphasized separately for both parts.

- ***Identification and Authentication:*** On the client-side, the TOE authenticates the client users using the PIN information of the user network access certificate (*SayTRUST Access Certificate*) before allowing access from remote public networks to the private network. Client users who want to access the private network must have the sayTRUST Access Client Application and a user network access certificate specially defined on the server part of the TOE (*sayTRUST Access Server OS*).

After the sayTRUST Access Client Application is run by clicking, it starts the server connection process to be able to establish a secure connection (*by using the Crypto Libraries*) to the private network. During the server connection process, the sayTRUST Access Client Application requests the PIN information of the SayTRUST Access Certificate from the client user. The client user must enter the PIN information on the PIN entry screen opening. To prevent a brute force attack, an incorrect PIN limit is applied.

On the server-side, the TOE provides an authentication mechanism to identify and authenticate administrators of the TOE *(System Administrator or Sub-Administrator*) and to enforce access control for the objects and functions of the TOE. The authentication mechanism is implemented with a username and password. The administrators of the TOE who want to access the sayTRUST Access Server for management activities enter their username and password via Web Browser. To prevent attacks, an incorrect password limit is applied, and inactive administrative sessions are automatically terminated after a preconfigured time. During password determination, the password of the administrators of the TOE is checked whether the password quality meets the defined quality measure.

- ***Security Management:*** The management functions on the server-side are provided via a Web Browser for the administrators associated with TOE's roles (*System Administrator and Sub-Administrator*) to manage the TOE according to their access privileges.

  On the client-side, after the server connection is successfully established, management functions are made available to client users via the user interface of the sayTRUST Access Client Application.

- ***Audit:*** All security-relevant events are logged with date and time information, type information of the event, the information whether the event was successful or failed, and the subject identity (*if applicable*).

  On the server-side logs for each day are stored in the file system automatically. These logs can be viewed and filtered by administrators of the TOE (*if they are authorized*) via a Web Browser. The TOE also restricts the ability to modify and delete the server audit log to unauthorized users.

  On the client-side, logs (*server connection activities, control activities of the processes running on PC RAM*) are stored temporarily. These logs can only be viewed on the user interface of the sayTRUST Access Client Application after server connection is active. Logs are deleted automatically after server connection session is disconnected. Client user can record (*if preferred*) to any location manually.

Cryptographic Support: Both on the client-side and on the server-side, crypto libraries perform all cryptographic operations such as TLS protocol implementation (*TLS v1.2 between TOE parts and TLS v1.2/TLS v1.3 for https connection with Web Browser*), cryptographic key generation, cryptographic operation (*encryption, decryption, hash calculation and digital signature & verification*), and key destruction.

1.3. Threats

This section identifies the threats to the assets.

Table 1: *Threats*

Threat	Definition
T. Unauthorized_Client	An attacker may try to gain unauthorized access to the private network.
T.Modify_Audit	An attacker or client users of the TOE could try to manipulate the audit data to hide its actions and unauthorized access attempts to the sayTRUST Access Server OS.
T.Untrusted_Channel	An attacker may attempt to disclose or modify the user data and TSF data transmitted between the TOE parts when traveling over an untrusted public network.
T.Malfunction	Due to a malfunction that an attacker may cause in the client part of the TOE (*such as corruption that will cause the TOE not to work as expected),* the transmitted user data may be modified or disclosed by an attacker.
T. Unauthorized _Admin	Any user inside the private network (*client user not authorized for the management activities*) may try to gain a management access.
T.Unauthorized_Manage	An attacker may attempt to disclose the authentication data of the administrators of the TOE transmitted via Web Browser to the sayTRUST Access Server OS and may attempt to modify administration session information (*management data*) for manipulation of the configuration of the sayTRUST Access Server OS

1.4. Organizational Security Policies (OSPs)

The TOE must satisfy the following objectives of the TOE.

Table 2: *Security Objectives of the TOE*

Objective	Definition
O.User_Definition	Users who want to access the private network with the sayTRUST Access Client Application must be defined on the sayTRUST Access Server OS and network access credentials (*sayTRUST Access Certificate along with PIN information*) must be created according to their network access privileges.
O.User_Authentication	The TOE shall provide authentication mechanism for client users to enable to private network access via the SayTRUST Access Client Application. The client user who wants to access to the private network must be authenticated with the PIN information of the sayTRUST Access Certificate.
O.Auth_Admin	The TOE shall provide a mechanism to authenticate TOE Administrators with username and password before accessing to the sayTRUST Access Server OS. To prevent attacks, an incorrect password limit must be applied, and inactive administrative sessions must be automatically terminated after a preconfigured time. During password determination, the password of the TOE Administrators must be checked whether the password quality meets the defined quality measure.
O.Secure_Comm	The TOE must communicate securely (*https connection using TLS v1.2/TLS v1.3 protocol*) with a Web Browser.
O.Key_Management	The TOE must provide the means for secure management of cryptographic keys used for secure messaging between TOE parts and secure communication with administrators of the TOE via Web Browser.
O.Roles	The sayTRUST Access Server OS must provide multiple administrative roles (*System Administrator and Sub-Administrators*) to isolate non-overlapping administrative

	function. The TOE must restrict its management functionality according to the access rights of the TOE Administrators. On the client-side, there is only one authorized role. sayTRUST Access Client Application must associate users with client user role after authentication process is success.
O.Audit_Gen	The TOE must record events of security relevance with accurate dates and timestamps. The TOE must provide authorized administrators (*on the server-side*) and client user (*on the client-side*) with the ability to review the audit records.
O.Audit_Protect	The TOE must protect the stored audit records on the server part of the TOE from unauthorized deletion and modifications in the audit trail.
O.Secure_Message	The TOE must communicate securely (*with TLS v1.2 Client Authentication*) to protect the user data and TSF data transmitted between separate parts of the TOE.

The TOE's IT environment must satisfy the following objectives.

Table 3: *Security Objectives for the Operational Environment*

Objective	Definition
OE.Physical_Protection	***It has to be ensured that*** the server on which the server part of the TOE is running is physically protected against unauthorized access or destruction.
OE.Trusted_Config	***It has to be ensured that*** the TOE Administrators (*System Administrator and Sub-Administrators*) are well trained and non-hostile. They read the guidance documentation carefully, completely understands and applies it.
OE.TOE_Environment	***It has to be ensured that*** the necessary infrastructure such as network devices and internet infrastructure are present in the environment in which the server part of the TOE runs. ***It has to be ensured that*** there are no viruses, Trojans and malware on both server-side and client-side (*on the USB Sticks*)
OE.Audit	***It has to be ensured that*** appropriate audit logs stored on the server side are regularly examined and backed up.

OE.Certificate_PIN	***It has to be ensured that*** the client user is informed about does not share the PIN information of the sayTRUST Access Certificate.
OE.Distribution	***Those responsible for the operation of the TOE must ensure that*** the user network access certificate and its PIN information are distributed to the client user using a secure way (*encrypted with a minimum AES 128-bit key or another method with equal security*).
OE.Fail_Safe	The TOE Environment must preserve a secure state if a self-test (*integrity test of the TSF*) of the client part of the TOE (*sayTRUST Access Client Application and Crypto Libraries)* error occurs during the initial start-up. If the TOE environment detects a problem with the integrity of the client part of the TOE, it must prevent the TOE from running.

1.5. Assumptions

These assumptions are made on the operational environment in order to be able to ensure that the security functionality can be provided by the TOE. If the TOE is placed in an operational environment that does not meet these assumptions, the TOE may no longer be able to provide all its security functionality.

The assumptions for the operational environment are given in Table 4.

Table 4: *Assumptions for the Operational Environment*

Assumption	Definition
A.Physical_Protection	***It is assumed that*** the server on which the server part of the TOE is running is physically protected against unauthorized access or destruction.
A.Trusted_Config	***It is assumed that*** the TOE Administrators (*System Administrator and Sub-Administrators*) are well trained and non-hostile. They read the guidance documentation carefully, completely understands and applies it.
A.Audit	***It is assumed that*** maintained audit logs are regularly examined and backed up periodically.

A.TOE_Environment	***It is assumed that*** the necessary infrastructure such as network devices and internet infrastructure are present in the environment in which the server part of the TOE runs. ***It is assumed that*** there are no viruses, Trojans and malware on both server-side and client-side (*on the USB Sticks*)
A. Certificate_PIN	***It is assumed that*** the client user who has the sayTRUST Access Client does not share the PIN information of the sayTRUST Access Certificate with anyone.

2 -CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-99
TOE Name and Version	sayTRUST Secure Access System v0.6
Security Target Title	sayTRUST Secure Access System Security Target
Security Target Version	3.6
Security Target Date	27/10/2025
Assurance Level	EAL 4+ (AVA_VAN.5)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2012-09-001, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1 Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2012-09-003, Version 3.1 Revision 5, April 2017
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2012-09-004, Version 3.1, Revision 5, April 2017
Protection Profile Conformance	None

Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, conformant • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, conformant
Sponsor	MİKROLİNK BİLİŞİM SAN. TİC. A.Ş.
Developer	SAYTEC SİBER SAVUNMA TEKNOLOJİLERİ A.Ş.
Evaluation Facility	BEAM TEKNOLOJİ A.Ş.
Certification Scheme	TSE CCCS

2.2 Security Policy

The following table describes the rationale for the *OSP* to security objectives mapping.

Table 1: *Objectives Mapping for OSPs*

OSP	Objectives	Rationale
P.Distribution	**OE.Distribution**	***OE.Distribution*** fulfils this policy by ensuring that the sayTRUST Access Certificate user network access certificate and its PIN information are distributed to the client user using a secure way (*encrypted with a minimum AES 128-bit key or another method with equal security*).

2.3 Assumptions and Clarification of Scope

The assumptions for the operational environment are given in Table 6.

Table 6: *Assumptions for the Operational Environment*

Assumption	Definition
A.Physical_Protection	***It is assumed that*** the server on which the server part of the TOE is running is physically protected against unauthorized access or destruction.
A.Trusted_Config	***It is assumed that*** the TOE Administrators (*System Administrator and Sub-Administrators*) are well trained and non-hostile. They read the guidance documentation carefully, completely understands and applies it.
A.Audit	***It is assumed that*** maintained audit logs are regularly examined and backed up periodically.
A.TOE_Environment	***It is assumed that*** the necessary infrastructure such as network devices and internet infrastructure are present in the environment in which the server part of the TOE runs. ***It is assumed that*** there are no viruses, Trojans and malware on both server-side and client-side (*on the USB Sticks*)
A. Certificate_PIN	***It is assumed that*** the client user who has the sayTRUST Access Client does not share the PIN information of the sayTRUST Access Certificate with anyone.

For further clarification of the scope, see related ST.

2.4 Architectural Information

The physical scope of the TOE consists of the components located in two separate locations (*as shown in Figure 1 with red dashed frame*) and TOE Documentations.

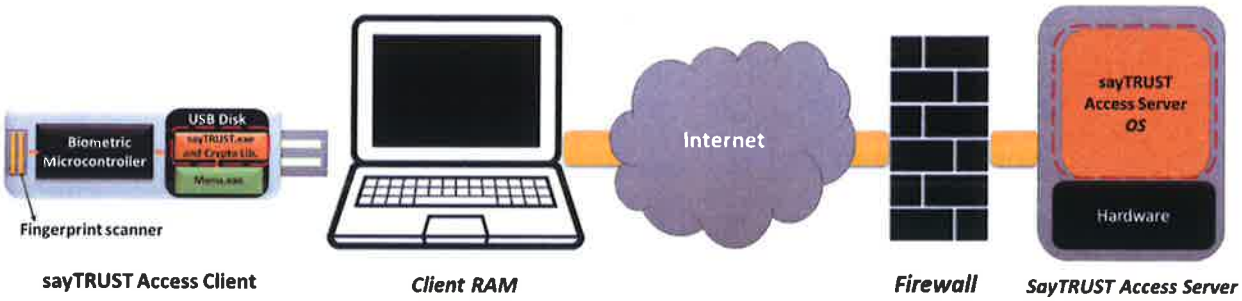

Figure 1: *The Physical Scope of the TOE*

Opposed to the traditional VPN solutions, the VPSC based SayTRUST® Access solution does not require installation and configuration on the client side. Therefore, users can securely connect to the working environment (*as in compliance with related authorizations*) from any computer (*meeting the requirement specified in ST*) via USB Sticks, according to their authorization. The VPSC based SayTRUST® Access solution consists of below components:

- ***sayTRUST Access Client v5.4***
  - *Biometric Microcontroller USB Client (not part of the TOE)*
  - *SayTRUST Access Menu v5.4.0.0 (not part of the TOE)*
    - ✓ *Menu.exe*
  - *sayTRUST Access Client Application v5.4.4.10 (part of the TOE)*
    - ✓ *sayTRUST.exe*
  - *Crypto Libraries v1.1.0k (part of the TOE)*
    - ✓ *libcrypto-1_1.dll*
    - ✓ *libssl-1_1.dll*
- ***sayTRUST Access Server***
  - *Server Hardware (not part of the TOE)*
  - *sayTRUST Access Server Operating System v4.6.22 (part of the TOE)*

sayTRUST Access Client represents the collection of Biometric Microcontroller USB Client, sayTRUST Client Application, sayTRUST Access Menu and Crypto Libraries. Its components in the physical scope of the TOE are described below.

- ***sayTRUST Client Application*** is application software that is stored on the USB Disk and used for client user remote access to the private network. After the secure connection (*TLS v1.2 Client Authentication*) is established between sayTRUST Access Server, it provides a user screen for the

client user for management activities. It uses the software crypto libraries for the TLS connection and cryptographic operations. It is checked whether this delivered part is the certified version or not, by comparing the version in the application details accessed by clicking the right mouse button and the version information in the ST.

- ***Crypto Libraries*** are software libraries written as open source using the C programming language and used for TLS connection and cryptographic operations. It is checked whether this delivered part is the certified version or not, by comparing the version in the application details accessed by clicking the right mouse button and the version information in the ST.

sayTRUST Access Server represents the collection of Server Hardware, sayTRUST Operating System. Its component in the physical scope of the TOE is described below.

- ***The sayTRUST Access Server OS*** is the first access point of clients who want to access the private network at the application level. Clients cannot access any services on the private network without authenticating themselves and establishing a secure connection.

Only users whose privileges are defined can contact this part of the TOE.

The registration of the client users to the sayTRUST Access Server OS is done by the administrators of the TOE *(System Administrator or Sub-Administrators (if they are authorized))* only through a local connection over the private network via the WEB GUI (*any web Bowser such as Firefox, Safari, Chrome or Internet Explorer*). It is not possible to access the administrative interface from the outside but if the secure connection is established via the sayTRUST Access Client Application, the TOE Users can access remotely to the login page via a Web Browser running on the Client PC (*using local IP/Port of the sayTRUST Access Server OS*).

The TOE administrator verifies himself/herself with the username and password through this WEB Browser. If the verification is successful, he will have administrative rights on the sayTRUST Access Server OS. By default, a single administrator (*System Administrator*) must be defined on the sayTRUST Access Server OS during installation and has full control over it but sub-administrators with lower privileges can be created by System Administrator.

If this part of the TOE will not be delivered to the customer installed on sayTRUST Access VPST Appliance, it is delivered (*in .iso format*) with Installation USB. The TOE is delivered to the customer's address by the company staff and is installed according to the TOE documentation. It is checked whether

this delivered part is certified versions or not, by comparing the version that appears on the initial setup screen and the version information in the ST.

TOE Documentation consists of:

- The TOE Operational Guidance
- The TOE Preparative Procedures

sayTEC AG customers may contact sayTRUST Enterprise support to request a copy of the guidance, which provides instructions and cautions for operating the product in its evaluated configuration.

For further architecture information, see related ST.

2.5 Documentation

Documents below are provided to the customer by the developer alongside the TOE:

Document Name	Version	Release Date
sayTRUST Secure Access System Security Target	v3.6	27/10/2025
Operational User Guidance	v1.6	08/08/2024
Preparative Procedures	v1.2	08/07/2024

2.6 IT Product Testing

During the evaluation, all evaluation evidences of TOE were delivered and transferred compeletely to CCTL by the developer. All the delivered evaluation evidences which include software, documents, etc. are mapped to the assurance families and the evaluation evidences has been established. The evaluation results are available at the final Evaluation Technical Report (ETR) of sayTRUST Secure Access System v0.6. It is concluded that the TOE supports EAL 4 augmented with AVA_VAN.5.

- **Developer Testing:** Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE design documentation which includes TSF subsystems and its interactions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 13 functional tests in total.
- **Evaluator Testing:** Evaluator has conducted 13 developer tests. Additionally, evaluator has prepared 10 independent tests. TOE has passed all functional tests to demonstrate that its security functions work as it is defined in the ST.

- **Penetration Tests:** TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 23 penetration tests have been conducted. TOE proved that it is resistant to "Attacker with High Attack Potential".

2.7 Evaluated Configuration

Evaluated TOE configuration is composed of:

- sayTRUST Secure Access System v0.6

Also as consistent with the minimum Hardware/ Software/ OS requirements for the TOE, the test environment presented at the ETR is composed of software and hardware.

2.8 Results of the Evaluation

The table below provides a complete list of the Security Assurance Requirements for the TOE. These requirements consist of the Evaluation Assurance Level 4 (EAL 4) components augmented with AVA_VAN.5 as specified in Part 3 of the Common Criteria.

Class Heading	Class Family	Description	Result
ADV: Development	ADV_ARC.1	Security architecture description	PASS
	ADV_FSP.4	Complete functional specification	PASS
	ADV_IMP.1	Implementation representation	PASS
	ADV_TDS.3	Basic modular design	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational user guidance	PASS
	AGD_PRE.1	Preparative procedures	PASS
ALC: Lifecycle Support	ALC_CMC.4	Production support, acceptance procedures and automation	PASS
	ALC_CMS.5	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery procedures	PASS
	ALC_DVS.1	Identification of security measures	PASS
	ALC_LCD.1	Developer-defined life-cycle model	PASS
	ALC_TAT.1	Well-defined development tools	PASS
ASE:	ASE_CCL.1	Conformance claims	PASS
	ASE_ECD.1	Extended components definition	PASS

Class Heading	Class Family	Description	Result
Security Target evaluation	ASE_INT.1	ST introduction	PASS
	ASE_OBJ.2	Security objectives	PASS
	ASE_REQ.2	Derived security requirements	PASS
	ASE_SPD.1	Security problem definition	PASS
	ASE_TSS.1	TOE summary specification	PASS
ATE: Tests	ATE_COV.1	Analysis of coverage	PASS
	ATE_DPT.1	Testing: basic design	PASS
	ATE_FUN.1	Functional testing	PASS
	ATE_IND.2	Independent testing - sample	PASS
AVA: Vulnerability Analysis	AVA_VAN.5	Focused vulnerability analysis	PASS

2.9 Evaluator Comments / Recommendations

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable with the stated security objectives for the operational environment and it can be suitably addressed.

3 SECURITY TARGET

The security target associated with this Certification Report is identified by the following terminology:

Title: sayTRUST Secure Access System Security Target

Version: v3.6

Date of Document: October 27, 2025

A public version has been created and verified according to ST-Sanitizing:

Title: sayTRUST Secure Access System Security Target

Version: v3.7

Date of Document: October 27, 2025

4 GLOSSARY

CCCS: Common Criteria Certification Scheme

CCMB: Common Criteria Management Board

CCRA: Common Criteria Recognition Arrangement

CKM: Cryptographic Key Management

COP: Cryptographic Operation

CR: Certification Report

EAL: Evaluation Assurance Level

FTP: Function of Trusted Path

IFC: Information Flow Control

IoT: Internet of Things

ITC: Inter TSF Confidentiality

MSA: Management of Security Attributes

OSP: Organizational Security Policy

OTA: Over the Air

SAR: Security Assurance Requirements

SFR: Security Functional Requirements

SHA: Secure Hash Algorithm

SMF: Specification of Management Functions

ST: Security Target

TLS: Transport Layer Security

TOE: Target of Evaluation

TDC: TSF Data Consistency

TSF: TOE Security Functionality

TSFI: TSF Interface

VPSC: Virtual Protected Secure Communication

5 BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1

Revision 5, April 2017

[3] BTTM-CCE-043 DTR v2.2 BTTM Evaluation Technical Report, Version 2.2, Rel. Date: December 10, 2024.

[4] sayTRUST Secure Access System Security Target, Version 3.6, Rel. Date: October 27, 2025.

[5] sayTRUST Secure Access System Security Target, Version 3.7, Rel. Date: October 27, 2025.

6 ANNEXES

6.1 TOE SPECIFICATIONS

TOE: sayTRUST Secure Access System v0.6

TOE Hash (SHA256):

Modules	**SHA-256**
sayTRUST Secure Access System v0.6	572A1CECBDE5E69F2EF2776A05AFA796D2199E59468871FBD07E19A19DC7B49D