eSTORM Co., Ltd.

AutoPassword Enterprise v4

Security Target v1.2

Revision history

Version	Date	Changes	Author
1.0	2025-07-07	Initial document	eSTORM Co., Ltd.
1.1	2025-09-18	Updated to reflect feedback	eSTORM Co., Ltd.
1.2	2025-11-06	Updated to reflect feedback	eSTORM Co., Ltd.

Table of contents

1 ST introduction

1.1 ST reference

Title	AutoPassword Enterprise v4 Security Target
Version	v1.2
Date	2025-11-06
Author	eSTORM Co., Ltd.
CC version	CC:2022 R1
Evaluation Assurance Level	EAL1

1.2 TOE reference

TOE	AutoPassword Enterprise v4
Version	v4.0.3
Components	AutoPassword Enterprise v4 Server v4.0.1 (autopassword_enterprise_v4_server_v4.0.1.tgz)
	AutoPassword Enterprise v4 Android App v4.0.1 (autopassword_enterprise_v4_android_app_v4.0.1.apk)
	AutoPassword Enterprise v4 iOS App v4.0.1 (autopassword_enterprise_v4_ios_app_v4.0.1.ipa)
Documents	AutoPassword Enterprise v4 Installation Manual v1.1 (AutoPassword Enterprise v4 Installation Manual v1.1.pdf)
	AutoPassword Enterprise v4 User Manual v1.1 (AutoPassword Enterprise v4 User Manual v1.1.pdf)
Developer	eSTORM Co., Ltd.

1.3 TOE overview

The Target of Evaluation (TOE) is an Out-of-Band (OOB) server authentication product. When a user accesses an online service provided by a business server, instead of using the traditional password entry method, the TOE utilizes the user's mobile device to provide secure mutual authentication between the business server and the user.

This system operates by first verifying the business server through an OOB channel using the AutoPassword Enterprise v4 Android/iOS App (hereafter "the authentication app") installed on the user's mobile device. This helps protect users from threats like phishing attacks and ensures they connect to a trusted online service.

The TOE's authentication process flows as follows:

1) **Server authentication**: When a user attempts to log into the business server's online service, the business server presents the user with server authentication information generated by the AutoPassword Enterprise v4 Server, rather than requesting a password.

2) **Comparison and verification**: The user compares the server authentication information presented by the business server with the server authentication information independently generated by the authentication app on their mobile device.

3) **Server trust confirmation**: If the two pieces of information match, the user confirms the authenticity of the business server and approves the connection through the authentication app.

4) **User authentication**: Once server authentication is complete, the authentication app generates user authentication information and sends it to the AutoPassword Enterprise v4 Server to complete the user's authentication.

5) **Service provision**: After the business server receives the authentication result from the AutoPassword Enterprise v4 Server, it provides the online service to the user.

The TOE consists of the following main components:

- **AutoPassword Enterprise v4 Server**: The server software responsible for the operation, management, and core security functions of the TOE system.
- **AutoPassword Enterprise v4 Android/iOS App**: The mobile app installed on the user's mobile device that generates and verifies the server/user authentication information.

The security functions for each TOE component are as follows.

AutoPassword Enterprise v4 Server

- **Security audit**: Generates, records, and manages audit data for key auditable activities.
- **Cryptographic support**: Manages cryptographic keys and performs cryptographic operations to encrypt communication between components and to protect the TSF (TOE Security Functionality) and TSF data.
- **Identification and authentication**: Identifies and authenticates the authorized system administrator; generates and verifies server/user authentication information.
- **Security management**: Defines security functions, administrator roles, and manages security policies.

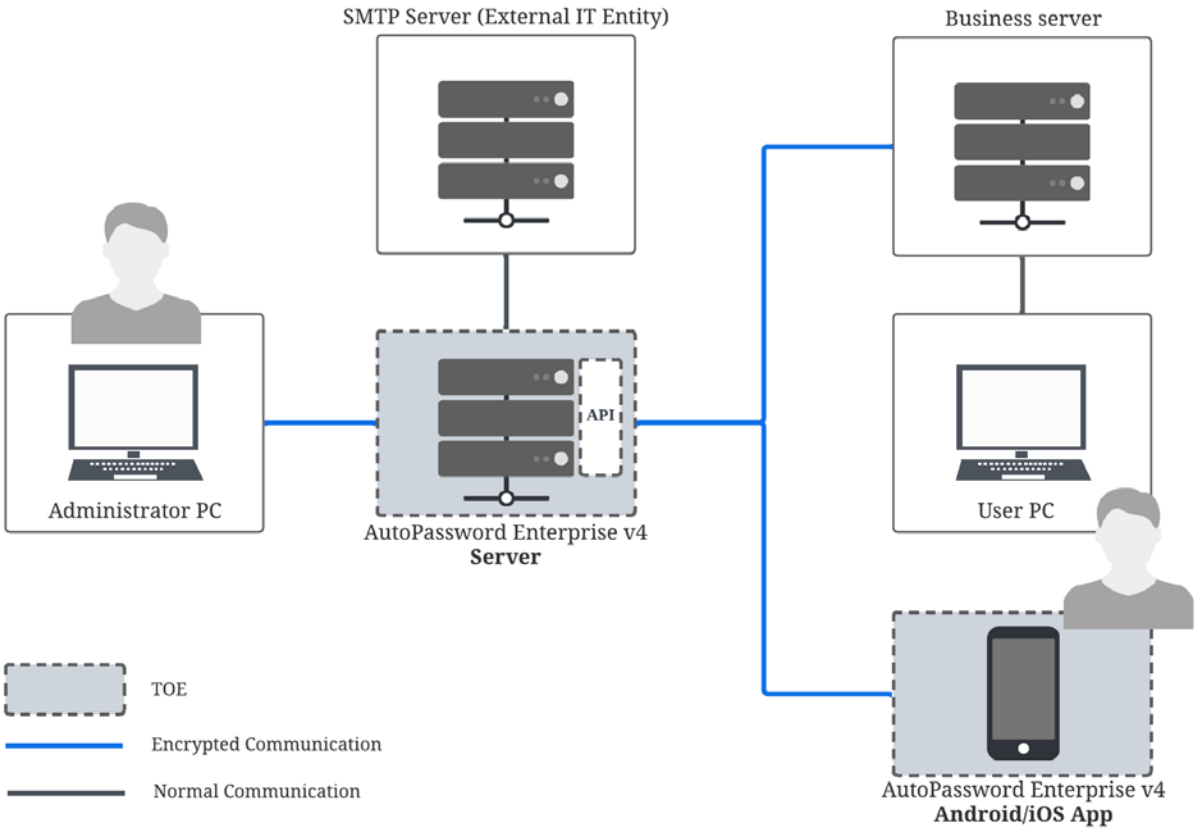
- **Protection of the TSF**: Protects data transmitted between components, protects stored TSF data, and performs TSF self-tests and integrity verification.
- **TOE access**: Manages secure sessions for the authorized administrator.

AutoPassword Enterprise v4 Android/iOS App

- **Security audit**: Pre-identifies key auditable activities and sends the corresponding audit data to the AutoPassword Enterprise v4 Server.
- **Cryptographic support**: Encrypts communication with the server and performs the cryptographic operations necessary to generate server and user authentication information.
- **Identification and authentication**: Generates and verifies server/user authentication information.
- **Protection of the TSF**: Protects data transmitted between components, protects stored TSF data, and performs TSF self-tests and integrity verification.

1.3.1 TOE operational environment

[Figure 1-1] below illustrates how the Target of Evaluation (TOE) components of the AutoPassword Enterprise v4 product family interact in a real-world environment. The TOE consists of the AutoPassword Enterprise v4 Server and the AutoPassword Enterprise v4 Android/iOS App.



[Figure 1-1] TOE operational environment

From an administrator's PC with an allowed IP address, the administrator accesses the AutoPassword Enterprise v4 Server's web management console via a web browser. After identification and authentication, they perform various security management tasks.

The user connects to the business server from a user's PC. During the authentication process, mutual authentication is performed by verifying the server authentication information and user authentication information, which are generated by the AutoPassword Enterprise v4 Server and the AutoPassword Enterprise v4 Android/iOS App, respectively.

The business server's online service is provided to user requests after authentication is complete. The SMTP server (an external IT entity) performs the function of sending alarm emails when a potential security violation is detected.

The TOE components are indicated by a dotted box in the diagram, and the blue lines represent encrypted communication channels.

1.3.2 Software/Hardware required for TOE operation

The minimum software and hardware specifications required for TOE operation are as follows in [Table 1-1].

AutoPassword Enterprise v4 Server	CPU	Intel(R) Core(TM) i5-13400 CPU @ 2.50 GHz or higher
	RAM	16 GB or higher
	DISK	10 GB or more of space required for TOE installation
	NIC	100/1000 Mbps 1 개 이상
	OS	Rocky Linux 8.10 64-bit (Kernel 4.18.0-553.62.1)
	S/W	MariaDB 10.11.14
		Tomcat 9.0.111
		OpenJDK 21.0.9_10
		NGINX 1.28.0
AutoPassword Enterprise v4 Android App	Product Name	Samsung Galaxy S23
	Model Number	SM-S911N
	OS	Android 16
	Kernel Version	5.15.41
AutoPassword Enterprise v4 iOS App	Product Name	iPhone 13
	Model Number	MLQ73KH/A
	OS	iOS 18
	Kernel Version	24.5.0

[Table 1-1] Minimum software/hardware specifications required for TOE operation

Web browser specification for the administrator for security management: Chrome 141.0 (64-bit)

The external IT entities required for TOE operation are as follows in [Table 1-2].

SMTP server	Sends an alarm email to the authorized administrator when a potential security violation is detected.

[Table 1-2] External IT entities required for TOE operation

1.4 TOE description

1.4.1 TOE physical scope

The TOE package is distributed in the form shown in [Table 1-3] below.

TOE	AutoPassword Enterprise v4
Version	v4.0.3

Category	Name (Filename)	Type	Distribution format
TOE components	AutoPassword Enterprise v4 Server v4.0.1 (autopassword_enterprise_v4_server_v4.0.1.tgz)	S/W	CD
	AutoPassword Enterprise v4 Android App v4.0.1 (autopassword_enterprise_v4_android_app_v4.0.1.apk)		
	AutoPassword Enterprise v4 iOS App v4.0.1 (autopassword_enterprise_v4_ios_app_v4.0.1.ipa)		
Documents	AutoPassword Enterprise v4 Installation Manual v1.1 (AutoPassword Enterprise v4 Installation Manual v1.1.pdf)	PDF	
	AutoPassword Enterprise v4 User Manual v1.1 (AutoPassword Enterprise v4 User Manual v1.1.pdf)		

[Table 1-3] TOE physical scope

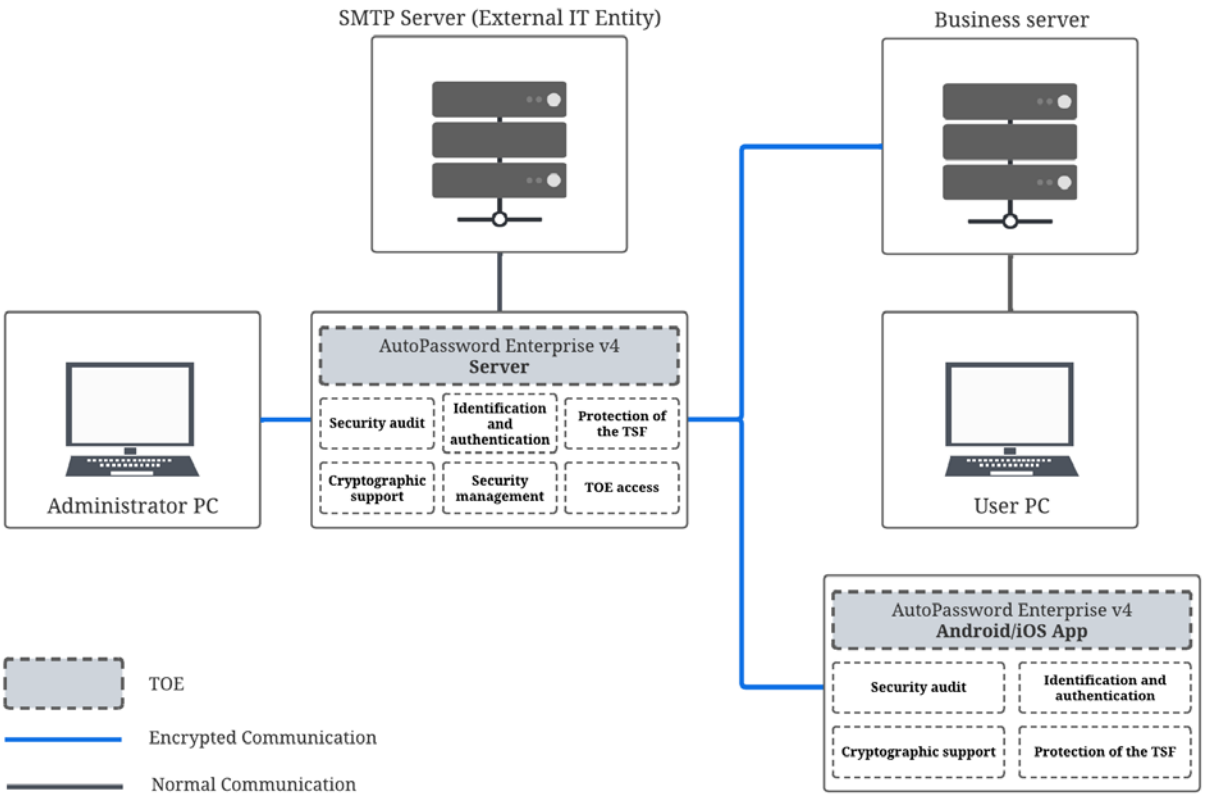
The 3rd party software included in the TOE is as follows in [Table 1-4].

AutoPassword Enterprise v4 Server	OpenSSL 3.0.18	TSF data encryption, communication channel encryption
AutoPassword Enterprise v4 Android App		
AutoPassword Enterprise v4 iOS App		

[Table 1-4] 3rd party software required for TOE operation

1.4.2 TOE logical scope

[Figure 1-2] below shows the logical scope of the TOE.



[Figure 1-2] TOE logical scope

AutoPassword Enterprise v4 Server main features

[Security audit]

The AutoPassword Enterprise v4 Server is designed to identify and record security-related events, enabling real-time detection of potential security violations and facilitating an effective response.

When situations like reaching the allowed number of authentication failures, self-test failures, integrity violations, or anticipated audit data loss occur, they are considered potential security violations. An alarm email is immediately sent to the administrator in these cases.

When an event occurs, the server automatically generates an audit record that includes the event's date and time, type, outcome (success or failure), and the subject's identity.

Generated audit records are provided in a user-friendly format. The authorized administrator can query and sort the audit data based on criteria such as keywords, date ranges, and event types.

Audit data is stored securely in an internal DBMS. An alarm email is sent to the administrator once each time the storage usage exceeds 60%, 70%, and 80% of its total allocated capacity.

When the storage is full, the oldest audit records are automatically overwritten. In this event, an alarm email is also sent to the administrator, allowing them to be aware of potential data loss in advance.

[Cryptographic support]

The AutoPassword Enterprise v4 Server provides various cryptographic functions based on standard technologies to encrypt communication channels between TOE components, protect server/user authentication information, protect sessions, and ensure the confidentiality and integrity of important stored data. These functions are implemented through proven cryptographic algorithms and secure key management procedures, covering the entire lifecycle of cryptographic keys from generation to destruction.

Cryptographic key generation is performed as follows. For TLS 1.2 communication, the server generates a 2048-bit RSA asymmetric key for server authentication and to verify the user authentication information from the AutoPassword Enterprise v4 Android/iOS App. It also generates a 256-bit ECDHE asymmetric key used for session key establishment. The encryption key for stored data, the encryption key for data transmitted between the server and the business server, and the encryption key for data transmitted between TOE components are all generated as 128-bit keys using HASH_DRBG (SHA512). The generation key for server/user authentication information is generated as a 160-bit key using HASH_DRBG (SHA512).

Cryptographic key distribution is as follows. During TLS 1.2 communication, the session key is securely distributed using the ECDHE method. The encryption key for data sent between the AutoPassword Enterprise v4 Server and the business server, and the key for data sent between TOE components, are distributed using RSA 2048 asymmetric encryption.

Cryptographic key derivation is as follows. A 128-bit AES key, used as a Key Encrypting Key (KEK), is derived using PBKDF2 (SHA512) with the user-input password and a 128-bit Salt value as inputs. A 256-bit AES session key is derived using a Key Derivation Function (KDF) with the client random, server random, and shared secret as parameters.

Cryptographic operations are performed using the following cryptographic algorithms.

Standard	Algorithm	Key Size	Purpose
ISO/IEC 29167-10:2017	AES-128-CBC	128-bit	Encryption/decryption of the stored data encryption key using a KEK
			Encryption/decryption of phone numbers and email addresses

			Encryption/decryption for delivering authentication elements and the server/user authentication information generation key to AutoPassword Enterprise v4 Android/iOS App
			Encryption/decryption when storing the server/user authentication information generation key
			Encryption/decryption of the private key password
			Encryption/decryption of DBMS connection information
			Encryption/decryption of the SMTP password
ISO/IEC 9797-2	HMAC-SHA256	256-bit	Mutual verification during communication with the AutoPassword Enterprise v4 Android/iOS App
			Generation of server/user authentication information
RFC 3447	RSA 2048	2048-bit	Digital signature generation and verification for the AutoPassword Enterprise v4 Android/iOS App
			Encryption/decryption of the secret key provided to the business server
			Server verification in TLS 1.2
RFC 5289	AES256-GCM	256-bit	TLS 1.2 communication encryption
ISO/IEC 10118-3:2004	SHA256	N/A	Hashing passwords for storage
			TOE integrity verification
	SHA384	N/A	Integrity check for data communicated between TOE components

To generate random bits for cryptographic key generation and other purposes, the TSF performs a deterministic random bit generation service using HASH_DRBG (SHA512) in accordance with NIST SP 800-90A Rev.1 after initialization with a seed. A TSF interface is used for this initialization and seeding.

The TSF updates the DRBG state by reseeding in accordance with NIST SP 800-90A Rev. 1 using the TSF interface getrandom(). This occurs under the following conditions: after 256 generations, when 1 hour has passed since the last seeding, or upon an error.

Furthermore, the TSF seeds the DRBG using the software-based TSF entropy source getrandom(), which provides at least 256 bits of min-entropy. To generate the entropy input for the derivation function defined in NIST SP 800-90A Rev. 1, it performs a Hashing operation on the inputs from TSF interfaces to ensure the final result also has at least 256 bits of min-entropy.

Cryptographic keys are securely destroyed immediately when their purpose is fulfilled or they are no longer needed. All cryptographic keys are made irrecoverable by overwriting their memory region with zeros either one or three times.

[Identification and authentication]

The AutoPassword Enterprise v4 Server provides secure identification and authentication functions to verify the identity of authorized users and administrators, and to restrict their access and use of security functions.

When a user attempts to authenticate, the entered password is visually protected (e.g., displayed as ● characters). If authentication fails, only the failure result is provided, ensuring that specific causes are not exposed externally.

For administrator authentication attempts, an account protection function is activated by detecting the number of consecutive failures. If authentication fails 5 consecutive times, authentication is blocked for 5 minutes, after which it is automatically released.

The administrator's password must meet the following complexity criteria, which include requirements for length, character combination, repetition limits, sequential character prohibition, and reuse prohibition:

- Length must be between 10 and 20 characters, inclusive.
- Must include at least one character from each of the following groups: English uppercase and lowercase letters, numbers, and special characters (@, $, !, %, *, #, ?, &).
- Prohibition of using 3 or more identical consecutive characters or numbers.
- Prohibition of using 4 or more sequential characters or numbers from a keyboard layout.
- Prohibition of using 4 or more sequential numbers.
- Prohibition of using 4 or more sequential alphabetic characters.

The server generates and verifies the server authentication information used for server authentication and the user authentication information used for user authentication. The server/user authentication information is securely generated and used via HMAC-SHA-256, AES-128-CBC, RSA2048, and SHA-256 cryptographic algorithms. The components required to generate server authentication information include the session ID of the client accessing the business server, generation time, the server/user authentication information generation key, IP address, and digital signature verification data. The components required to generate user authentication information include the IP address of the AutoPassword Enterprise v4 Android/iOS App, the session ID of the client accessing the business server, the current time, the server/user authentication information generation key, and digital signature verification data.

During the authentication process, a unique random value is generated for each session to prevent the reuse of authentication data. This applies to administrator, server, and user authentication.

[Security management]

The AutoPassword Enterprise v4 Server provides a variety of management functions to securely operate its security features and related data. These functions are designed to be performed only by an authorized administrator.

The administrator can perform account management tasks such as registering, deleting, and modifying user and administrator accounts. They can also manage functions like setting up authenticators for each user, registering, deleting, and modifying integrated services, and issuing and renewing related keys.

Session-related security functions, such as resetting the user authentication failure count and releasing locked sessions, are also controlled through administrator privileges.

Audit records and authentication logs can only be viewed by the administrator, allowing them to track the system's operational status and security incidents.

The administrator can configure the IP addresses allowed to access the web management console and set up the SMTP server and alarm recipient email addresses.

At the administrator's request, an integrity check of the TOE's settings and executable code can be performed.

A function is provided to set the administrator ID and initial password during installation.

The server securely manages various internal security-related data, including identification information, authentication information, log data, and alarm settings for administrators, users, and integrated services. Access to and modification of this data is permitted only for the administrator.

The server performs access control for each management function based on the administrator's security role. There is only one administrator role, and only one administrator account exists. The administrator privileges include the following:

- Register and modify the administrator
- Register, delete, and modify users
- Register and delete authenticators for each user
- Register, delete, and modify integrated services
- Issue and renew integrated service keys
- Reset the user authentication failure count
- Unlock user sessions

- View audit records
- Set allowed IP addresses for web management console access
- Set credentials for accessing external IT entities
- Perform an integrity check of TOE settings and the TOE itself upon administrator request

[Protection of the TSF]

The AutoPassword Enterprise v4 Server provides various Protection of the TSF mechanisms to ensure the reliability of its security functions and to maintain the system's own integrity and stability.

It preserves a secure state even if a failure occurs during the generation of server/user authentication information. The process is safely terminated to prevent the error from affecting the entire system.

When TSF data is transmitted between TOE components, it is protected from unauthorized disclosure or modification. TSF data is always transmitted through a secure path.

Sensitive TSF data—such as the asymmetric key for server authentication in TLS 1.2, the asymmetric key for verifying user authentication information from the App, the stored data encryption key, the encryption key for data transmitted between the Server and the business server, the encryption key for data transmitted between TOE components, the server/user authentication information generation key, TOE settings stored in the DBMS, the private key password, the SMTP password, DBMS connection information, the administrator password, and audit data—is protected from unauthorized disclosure and modification when stored.

The server automatically performs self-tests and integrity verification during start-up and continues to perform them periodically during normal operation. The administrator can also initiate an integrity check of the server upon request.

[TOE access]

The AutoPassword Enterprise v4 Server limits the number of administrator sessions and their connection conditions to prevent the misuse of system resources and ensure secure access to the management interface.

Only a single session is permitted for the same administrator account; multiple concurrent sessions cannot be maintained. This prevents security threats such as session hijacking and duplicate logins.

After an administrator logs in, the session is automatically terminated if there is no activity for 10 minutes. This minimizes the security risks caused by unnecessarily open sessions.

Session establishment is controlled based on the connecting IP address. Attempts to access the management console from an unregistered IP address are blocked. This proactively prevents access from untrusted locations.

AutoPassword Enterprise v4 Android/iOS App main features

[Security audit]

The AutoPassword Enterprise v4 Android/iOS App identifies auditable events, such as identification and authentication, self-tests, and integrity verification, and transmits the audit data to the AutoPassword Enterprise v4 Server to be recorded.

[Cryptographic support]

The AutoPassword Enterprise v4 Android/iOS App provides cryptographic support functions to encrypt the communication channel between TOE components and to generate and protect user identification and authentication information.

It generates server/user authentication information, which is protected through AES-based encryption and digital signature algorithms. The generation key for this information is securely created according to a standard-based key derivation method.

[Identification and authentication]

The AutoPassword Enterprise v4 Android/iOS App generates and verifies the server authentication information used for server authentication and the user authentication information used for user authentication. The server/user authentication information is securely generated and used via HMAC-SHA-256, AES-128-CBC, RSA2048, and SHA-256 cryptographic algorithms. The components required to generate server authentication information include the session ID of the client accessing the business server, generation time, the server/user authentication information generation key, IP address, and digital signature verification data. The components required to generate user authentication information include the IP address of the App, the session ID of the client accessing the business server, the current time, the server/user authentication information generation key, and digital signature verification data.

During the authentication process, a unique random value (nonce) is generated for each session to prevent the reuse of authentication data, which applies to both server and user authentication.

[Protection of the TSF]

The AutoPassword Enterprise v4 Android/iOS App provides various TSF protection mechanisms to ensure the reliability of its security functions and to maintain its integrity and stability.

When TSF data is transmitted between TOE components, it is protected from unauthorized disclosure or modification. TSF data is always transmitted through a secure path.

Sensitive TSF data—such as the asymmetric key for server authentication in TLS 1.2, the asymmetric key for verifying user authentication information from the App, the stored data encryption key, the encryption key for data transmitted between TOE components, the server/user authentication information generation key, the private key password, and audit data—is protected from unauthorized disclosure and modification when stored.

The AutoPassword Enterprise v4 Android/iOS App automatically performs self-tests and integrity verification during start-up.

1.5 Conventions

The following operations are used in this Security Target.

Iteration

This is used when a single component is repeated multiple times to apply an operation in various ways. The result of an iteration is indicated by an iteration number in parentheses after the component identifier, i.e., (iteration number).

Assignment

This is used to assign a specific value to an unspecified parameter (e.g., password length). The result of an assignment is indicated by square brackets, i.e., [assigned value].

Selection

This is used to select one or more of the choices provided in the Common Criteria when describing a requirement. The result of a selection is indicated by *underlined italics*.

Refinement

This is used to make a requirement more restrictive by adding details. The result of a refinement is indicated by **bold text**.

1.6 Terms and definitions

Assignment

The specification of an identified parameter in a component (of the CC) or requirement

Authorized Administrator

Authorized user to securely operate and manage the TOE

Class

Set of CC families that share a common focus

Component

Smallest selectable set of elements on which requirements may be based

Dependency

Relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package

Element

Indivisible statement of a security need

Encryption

The act that converting the plaintext into the ciphertext using the encryption key

Evaluation Assurance Level (EAL)

Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package

External Entity

An entity (person or IT system) outside the TOE that interacts or may interact with the TOE

Family

Set of components that share a similar goal but differ in emphasis or rigo

Identity

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

Iteration

Use of the same component to express two or more distinct requirements

Operation (on a component of the CC)

Modification or repetition of a component. Allowed operations on components are assignment, iteration, refinement and selection

Operation (on a subject)

Specific type of action performed by a subject on an object

Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type

Refinement

Addition of details to a component

Role

Predefined set of rules on permissible interactions between a user and the TOE

Security Target (ST)

Implementation-dependent statement of security needs for a specific identified TOE

Selection

Specification of one or more items from a list in a component

Subject

Active entity in the TOE that performs operations on objects

Target of Evaluation (TOE)

Set of software, firmware and/or hardware possibly accompanied by guidance

TOE Security Functionality (TSF)

Combined functionality of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs

TSF Data

Data for the operation of the TOE upon which the enforcement of the SFR relies

1.7 ST structure

This Security Target describes the ST introduction, conformance claims, security problem definition, security objectives, security requirements, and the TOE summary specification.

1) The ST introduction describes the ST reference, TOE reference, TOE overview, and TOE description.
2) The conformance claims declare and describe conformance to the Common Criteria, security specifications, and packages.

3) Security objectives for the operational environment are defined to ensure that the TOE's security functionality is supported and can be provided correctly.

4) The extended components definition describes new extended components that are not included in Part 2 or Part 3 of the Common Criteria.

5) The security requirements section describes the security functional requirements (SFRs) and security assurance requirements (SARs).

6) The TOE summary specification describes how the security functional requirements are implemented in the TOE.

2 Conformance claims

2.1 CC conformance claim

Common Criteria		Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1 • Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, CC:2022 Revision 1 (CCMB-2022-11-001, November 2022) • Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, CC:2022 Revision 1 (CCMB-2022-11-002, November 2022) • Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, CC:2022 Revision 1 (CCMB-2022-11-003, November 2022) • Common Criteria for Information Technology Security Evaluation Part 4: Framework for the specification of evaluation methods and activities, CC:2022 Revision 1 (CCMB-2022-11-004, November 2022) • Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements, CC:2022 Revision 1 (CCMB-2022-11-005, November 2022)
Conformance Type	Part 2 Security functional components	Extended: FMT_PWD.1, FPT_PST.1
	Part 3 Security assurance components	Conformant
	Package	EAL1 conformant

2.2 PP conformance claim

This Security Target does not claim conformance to any Protection Profile.

2.3 Package conformance claim

This Security Target claims conformance to the assurance requirements package EAL1.

2.4 Conformance claim rationale

Since this Security Target does not claim conformance to any Protection Profile, a conformance claim rationale is not applicable.

2.5 Reference to evaluation methods/activities

This Security Target uses the evaluation methods and activities defined in section 6.2.1; there are no additional evaluation methods or activities.

3 Security problem definition

3.1 Assets

The primary assets to be protected by the TOE are as follows:

- Authentication data and user information
- The TOE itself and critical data related to TOE operation (e.g., TSF data)

3.2 Threats

Threat agents are IT entities and users who may harm the assets to be protected through unauthorized access or abnormal methods, and they can cause various threats as follows. The threat agents for the TOE are assumed to have a basic level of expertise, resources, and motivation.

3.2.1 Unauthorized access and data leakage

T.SESSION_HIJACK
A threat agent may hijack a user's privileges by accessing an unattended user screen that is still logged in, or by using a user session that has not been terminated after logout.

T.RETRY_AUTH_ATTEMPT
A threat agent may succeed in authentication by using information acquired through repeated authentication attempts, and then access the TOE by impersonating an authorized user.

T.IMPERSONATION
A threat agent may access the TOE by impersonating an authorized user, TOE component, or other entities.

T.REPLAY
A threat agent may discover and copy authentication information and reuse it to access the TOE.

T.WEAK_PASSWORD
A threat agent may acquire a poorly managed password (e.g., using dictionary words) to access the TOE by impersonating an authorized user, or may access the TOE by impersonating an authorized user if weak password policies are applied.

3.2.2 Information leakage

T.UNAUTHORIZED_INFO_LEAK
A threat agent may leak critical user information stored in the database through unauthorized means.

T.STORED_DATA_LEAKAGE
A threat agent may leak critical data (e.g., cryptographic keys, TOE settings) stored inside the TOE or in external entities interacting with the TOE (e.g., DBMS) through unauthorized means.

T.TRANSMISSION_DATA_DAMAGE
A threat agent may disclose or modify data transmitted between TOE components and with external IT entities through unauthorized means.

T.WEAK_CRYPTO_PROTOCOLS
A threat agent may analyze traffic that uses weak cryptographic protocols or low cryptographic strength to deduce key information or determine the content of encrypted communications.

3.2.3 TOE function compromise

T.TSF_COMPROMISE
A threat agent may compromise the TSF through unauthorized access, causing a malfunction of TOE functions or disabling them entirely.

3.3 Organizational security policies

P.AUDIT
To trace responsibility for security-related actions, security-relevant events must be recorded and maintained, and the recorded data must be reviewed. Furthermore, the available space on the audit data storage disk must be regularly checked to prevent data loss, and stored audit data must be protected from unauthorized modification and deletion.

P.SECURE_OPERATION
The TOE must provide administrative measures to allow the administrator to securely configure the TOE in compliance with the organization's security policies and to operate it correctly according to the TOE operational manuals.

P.CRYPTO_STRENGTH
The organization must apply encryption measures for the storage and transmission of critical data, such as passwords for user authentication, and must use secure cryptographic algorithms.

3.4 Assumptions

The following conditions are assumed to exist in the operational environment of a TOE conforming to this Security Target.

A.PHYSICAL_CONTROL
The location where the TOE is installed and operated must be equipped with access control and protective facilities to ensure that only authorized administrators can access it.

A.TRUSTED_ADMIN
The authorized administrators of the TOE are assumed to be non-malicious, appropriately trained on the TOE's administrative functions, and will perform their duties correctly in accordance with the administrator guidance.

A.SECURE_DEVELOPMENT
Developers who integrate user identification and authentication functions in the business server's operational environment using the TOE must comply with the requirements of the provided manuals to ensure the TOE's security functions are applied securely.

A.OPERATION_SYSTEM_REINFORCEMENT
The operating system on which the TOE is installed and operated must be hardened against the latest vulnerabilities to ensure its reliability and security.

A.SECURE_ADMIN_ACCESS
The web server, which is the administrative server's operational environment, and the web browser on the administrator's PC must communicate using a secure path.

4 Security objectives

The following security objectives for the operational environment must be addressed by technical or procedural means supported by the operational environment to ensure that the TOE can provide its security functionality correctly.

4.1 Security objectives for the operational environment

OE.LOG_BACKUP
To prepare for the loss of audit records, the TOE's authorized administrator must periodically check the available space in the audit data storage and perform audit record backups (e.g., to an external log server or a separate storage device) to prevent data loss.

OE.PHYSICAL_CONTROL
The location where the TOE is installed and operated must be equipped with access control and protective facilities to ensure that only authorized administrators can access it.

OE.TRUSTED_ADMIN
The authorized administrators of the TOE are assumed to be non-malicious, appropriately trained on the TOE's administrative functions, and will perform their duties correctly in accordance with the administrator guidance.

OE.SECURE_DEVELOPMENT
Developers who integrate user identification and authentication functions in the business server's operational environment using the TOE must comply with the requirements of the provided manuals to ensure the TOE's security functions are applied securely.

OE.OPERATION_SYSTEM_REINFORCEMENT
The operating system on which the TOE is installed and operated must be hardened against the latest vulnerabilities to ensure its reliability and security.

OE.TIMESTAMP
The TOE must use a reliable time stamp provided by the TOE operational environment to accurately record security-relevant events.

OE.SECURE_ACCESS
The confidentiality and integrity of data transmitted during communication between the administrator's PC web browser and the web server, which is the administrative server's operational environment, must be ensured.

OE.DBMS

The DBMS must securely store and protect the audit data and TSF data generated by the TOE.

4.2 Security objectives rationale

4.2.1 Rationale for the security objectives for the operational environment

	OE. LOG_BACKUP	OE. PHYSICAL_CONTROL	OE. TRUSTED_ADMIN	OE. SECURE_DEVELOPMENT	OE. OPERATION_SYSTEM_REINFORCEMENT	OE. TIMESTAMP	OE. SECURE_ACCESS	OE. DBMS
P. AUDIT	O					O		O
P. SECURE_OPERATION			O					
A. PHYSICAL_CONTROL		O						
A. TRUSTED_ADMIN	O		O					
A. SECURE_DEVELOPMENT				O				
A. OPERATION_SYSTEM_REINFORCEMENT					O			
A. SECURE_ADMIN_ACCESS							O	

P.AUDIT	OE.LOG_BACKUP, OE.TIMESTAMP, OE.DBMS
P.AUDIT is met by **OE.LOG_BACKUP**, **OE.TIMESTAMP**, and **OE.DBMS**. **OE.LOG_BACKUP** ensures that, in addition to the TOE's functions, the administrator periodically checks the available audit data storage space and performs regular log backups or sends logs to an external log server to prevent data loss. **OE.TIMESTAMP** ensures that the TOE accurately records security-relevant events using a reliable time stamp provided by the TOE operational environment. **OE.DBMS** ensures that the audit data generated by the TOE is securely stored in a reliable storage space, preventing the loss or alteration of audit data.	

P.SECURE_OPERATION	OE.TRUSTED_ADMIN
P.SECURE_OPERATION is met by **OE.TRUSTED_ADMIN**.	

OE.TRUSTED_ADMIN ensures that the administrator operates the TOE correctly according to the organizational security policies and operational manuals.

A.PHYSICAL_CONTROL	OE.PHYSICAL_CONTROL

A.PHYSICAL_CONTROL is supported by **OE.PHYSICAL_CONTROL**.

OE.PHYSICAL_CONTROL ensures that the administrative server is placed in a location with protective facilities and that access is controlled so only authorized administrators can enter.

A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN, OE.LOG_BACKUP

A.TRUSTED_ADMIN is supported by **OE.TRUSTED_ADMIN** and **OE.LOG_BACKUP**.

OE.TRUSTED_ADMIN ensures that the authorized administrators of the TOE are non-malicious, appropriately trained on the TOE's administrative functions, and will perform their duties correctly in accordance with the administrator guidance.

OE.LOG_BACKUP ensures that the authorized administrator periodically checks the available space in the audit data storage and performs audit record backups (e.g., to an external log server or a separate storage device) to prevent data exhaustion and loss.

A.SECURE_DEVELOPMENT	OE.SECURE_DEVELOPMENT

A.SECURE_DEVELOPMENT is supported by **OE.SECURE_DEVELOPMENT**.

OE.SECURE_DEVELOPMENT ensures that developers who integrate user identification and authentication functions in the business server's operational environment using the TOE comply with the requirements of the provided manuals to ensure the TOE's security functions are applied securely.

A.OPERATION_SYSTEM_REINFORCEMENT	OE.OPERATION_SYSTEM_REINFORCEMENT

A.OPERATION_SYSTEM_REINFORCEMENT is supported by **OE.OPERATION_SYSTEM_REINFORCEMENT**.

OE.OPERATION_SYSTEM_REINFORCEMENT ensures that the operating system on which the TOE is installed and operated is hardened against the latest vulnerabilities to ensure its reliability and security.

A.SECURE_ADMIN_ACCESS	OE.SECURE_ACCESS

A.SECURE_ADMIN_ACCESS is supported by **OE.SECURE_ACCESS**.

OE.SECURE_ACCESS ensures that communication between the administrator's PC web browser and the web server, which is the administrative server's operational environment, uses a secure path to guarantee the confidentiality and integrity of the transmitted data.

5 Extended components definition

5.1 Security management

5.1.1 ID and password

Family Behaviour

This family defines the capability that is required to control ID and password management used in the TOE, and set or modify ID and/or password by authorized users.

Components leveling and description

FMT_PWD.1 ID and password management, requires that the TSF provides the management function of ID and password.

Management of FMT_PWD.1

The following actions could be considered for the management functions in FMT:

a) management of ID and password configuration rules.

Audit of FMT_PWD.1

The following actions are recommended to record if FAU_GEN Security audit data generation is included in the ST:

a) minimal: All changes of the password.

FMT_PWD.1 Management of ID and password

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

1. [assignment: *password combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for password, etc.*]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [assignment: *list of functions*] to [assignment: *the authorized identified roles*].

1. [assignment: *ID combination rules and/or length*]
2. [assignment: *other management such as management of special characters unusable for ID, etc.*]

FMT_PWD.1.3 The TSF shall provide the capability for [selection, choose one of: *setting ID and password when installing, setting password when installing, changing the ID and password when the authorized administrator accesses for the first time, changing the password when the authorized administrator accesses for the first time*].

5.2 Protection of the TSF

5.2.1 Protection of stored TSF data

Family Behaviour

This family defines rules to protect TSF data stored within containers controlled by the TSF from the unauthorized modification or disclosure.

Components leveling and description

FPT_PST.1 Basic protection of stored TSF data requires the protection of TSF data stored in containers controlled by the TSF.

Management of FPT_PST.1

a) There are no management activities foreseen.

Audit of FPT_PST.1

a) There are no auditable events foreseen.

FPT_PST.1 Basic protection of stored TSF data

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PST.1.1 The TSF shall protect [assignment: *TSF data*] stored in containers controlled by the TSF from the unauthorized [selection: *disclosure, modification*].

6 Security requirements

The security requirements describe the functional and assurance requirements that must be satisfied by the TOE.

6.1 Security functional requirements

The security functional requirements are expressed by selecting relevant security functional components from Common Criteria Part 2 to satisfy the security objectives. [Table 6-1] lists the TOE security functional requirement components.

Class	Security functional components	
Security audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Audit data storage location
	FAU_STG.4	Action in case of possible audit data loss
	FAU_STG.5	Prevention of audit data loss
Cryptographic support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key distribution
	FCS_CKM.5	Cryptographic key derivation
	FCS_CKM.6	Timing and event of cryptographic key destruction
	FCS_COP.1	Cryptographic operation
	FCS_RBG.1	Random bit generation (RBG)
	FCS_RBG.3	Random bit generation (internal seeding – single source)
	FCS_RBG.5	Random bit generation (combining entropy sources)
Identification and authentication	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_SOS.2	TSF Generation of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security management	FMT_MOF.1	Management of security functions behaviour
	FMT_MTD.1	Management of TSF data
	FMT_PWD.1	Management of ID and password (Extended)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
	FPT_FLS.1	Failure with preservation of secure state

Protection of the TSF	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_PST.1	Basic protection of stored TSF data (Extended)
	FPT_TST.1	TSF self-testing
TOE access	FTA_MCS.2	Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.3	TSF-initiated termination
	FTA_TSE.1	TOE session establishment

[Table 6-1] TOE security functional requirement components

6.1.1 Security audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [send an alarm email to an email address registered by the authorized administrator] upon detection of a potential security violation.

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate audit data of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the *not specified* level of audit;

c) [See 'Auditable Events' in [Table 6-2]]

FAU_GEN.1.2 The TSF shall record within the audit data at least the following information:

a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;

b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [See 'Additional Audit Record Contents' in [Table 6-2]].

Security Functional Component	Auditable Event	Additional Audit Record Contents
FAU_ARP.1	Actions taken due to potential security violations	

FAU_GEN.1	None	
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms	
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.3	The parameters used for the viewing	
FAU_STG.1	None	
FAU_STG.4	Actions taken due to exceeding of a threshold	
FAU_STG.5	Actions taken due to the audit data storage failure	
FCS_CKM.1	Success and failure of the activity	
FCS_CKM.2	Success and failure of the activity	
FCS_CKM.5	Success and failure of the activity	
FCS_CKM.6	Success and failure of the activity	
FCS_COP.1	Success and failure, and the type of cryptographic operation	
FCS_RBG.1	Failure of the randomization process, failure to initialize or reseed	
FCS_RBG.3	None	
FCS_RBG.5	None	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.	
FIA_SOS.1	Rejection by the TSF of any tested secret	
FIA_SOS.2	Rejection by the TSF of any tested secret	
FIA_UAU.2	Unsuccessful use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UAU.7	None	
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
FMT_MTD.1	All modifications to the values of TSF data	Modified TSF data value
FMT_PWD.1	All modifications to the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the group of users that are part of a role	
FPT_FLS.1	Failure of the TSF	
FPT_ITT.1	None	
FPT_PST.1	None	
FPT_TST.1	Execution of the TSF self-tests and the results of the tests	Modified TSF data or executable

		code in case of integrity violation
FTA_MCS.2	Rejection of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.3	Termination of an interactive session by the session locking mechanism	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	

[Table 6-2] List of Auditable Events

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [reaching the threshold of failed authentication attempts (FIA_AFL.1), self-test failure (FPT_TST.1), integrity violation, exceeding the audit data storage threshold (FAU_STG.4), and overwriting the oldest audit record (FAU_STG.5)] known to indicate a potential security violation;

b) [None]

FAU_SAR.1 Audit review

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [the authorized administrator] with the capability to read [all audit data] from the audit data.

FAU_SAR.1.2 The TSF shall provide the audit data in a manner suitable for the **authorized administrator** to interpret the information.

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [the methods of selection and ordering specified in [Table 6-3]] of audit data based on [the following criteria with logical relations].

Audit Data Item	Search (with full AND or OR logic)	Sort (ascending/descending)
Keyword	○	○
Period	○	○
Event	○	○
Type	○	○

[Table 6-3] Search and Sort Functions per TOE Audit Data Item

FAU_STG.1 Audit data storage location

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FTP_ITC.1 Inter-TSF trusted channel

FAU_STG.1.1 The TSF shall be able to store generated audit data on the *[DMBS]*.

FAU_STG.4 Action in case of possible audit data loss

Hierarchical to: No other components.
Dependencies: FAU_STG.2 Protected audit data storage

FAU_STG.4.1 The TSF shall [send an alarm email once for each threshold range to the email address registered by the authorized administrator] if the audit data storage exceeds [60%, 70%, and 80% of its allocated capacity].

FAU_STG.5 Prevention of audit data loss

Hierarchical to: FAU_STG.4 Action in case of possible audit data loss

Dependencies: FAU_STG.2 Protected audit data storage

FAU_STG.5.1 The TSF shall *overwrite the oldest stored audit records*, [send an alarm email to the email address registered by the authorized administrator] if the audit data storage is full.

6.1.2 Cryptographic support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_CKM.5 Cryptographic key derivation, or
FCS_COP.1 Cryptographic operation]
[FCS_RBG.1 Random bit generation, or
FCS_RNG.1 Generation of random numbers]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [the 'Algorithm' column in [Table 6-4]] and specified cryptographic key sizes [the 'Key Size' column in [Table 6-4]] that meet the following: [the 'Standard' column in [Table 6-4]].

Standard	Algorithm	Key Size	Purpose
ISO/IEC 18033-2-2226	RSA 2048	2048-bit	Asymmetric key for server authentication during TLS 1.2 communication
			Asymmetric key to verify user authentication information from the AutoPassword Enterprise v4 Android/iOS App
ISO/IEC 18033-2:2006	ECDHE	256-bit	Asymmetric key for session key generation during TLS 1.2 communication
NIST SP 800-90A Rev.1	HASH_DRBG (SHA512)	128-bit	Stored data encryption key
			Encryption key for data transmitted between the

			AutoPassword Enterprise v4 Server and the business server
			Encryption key for data transmitted between TOE components
		160-bit	Generation key for server/user authentication information

[Table 6-4] Cryptographic Key Generation

FCS_CKM.2 Cryptographic key distribution

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation or
FCS_CKM.5 Cryptographic key derivation]

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [the 'Distribution Method' column in [Table 6-5]] that meets the following: [the 'Standard' column in [Table 6-5]].

Standard	Distribution Method	Purpose
ISO/IEC 18033-2:2006	ECDHE	Session key distribution for TLS 1.2 communication
ISO/IEC 18033-2-2226	RSA 2048	Distribution of the encryption key for data transmitted between the AutoPassword Enterprise v4 Server and the business server
		Distribution of the encryption key for data transmitted between TOE components

[Table 6-5] Cryptographic Key Distribution

FCS_CKM.5 Cryptographic key derivation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.5.1 The TSF shall derive cryptographic keys [the 'Key Type' column in [Table 6-6]] from [the 'Input Parameters' column in [Table 6-6]] in accordance with a specified key derivation algorithm [the 'Key Derivation Algorithm' column in [Table 6-6]] and specified cryptographic key sizes [the 'Key Size' column in [Table 6-6]] that meet the following: [the 'Standard' column in [Table 6-6]].

Standard	Key Derivation Algorithm	Key Size	Input Parameters	Key Type	Purpose
TTAK.KO-12.0334	PBKDF2 (SHA512)	128-bit	KEK password input by user	AES_128	KEK derivation for TOE components
			Salt(128-bit)		
ISO/IEC 11770-3	KDF	256-bit	Client random	AES_256	Session key derivation
			Server random		
			Shared secret		

[Table 6-6] Cryptographic Key Derivation

FCS_CKM.6 Timing and event of cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.5 Cryptographic key derivation]

FCS_CKM.6.1 The TSF shall destroy [the 'Cryptographic Key' column in [Table 6-7]] when *no longer needed*.

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [the 'Destruction Method' column in [Table 6-7]] that meets the following: [None].

Cryptographic Key	Destruction Method	Point of Destruction
Stored data encryption key	Overwrite memory with zero three times	Upon process termination

KEK (Key Encryption Key)	Overwrite memory with zero three times	Immediately after use
Key used during TLS 1.2 communication (Session key)	Overwrite memory with zero one time	Upon session termination
Key used during TLS 1.2 communication (Shared secret, secp256r1 asymmetric key, RSA2048 asymmetric key)	Overwrite memory with zero one time	After TLS 1.2 handshake completion
Encryption key for data transmitted between the AutoPassword Enterprise v4 Server and the business server	Overwrite memory with zero three times	Immediately after use
Encryption key for data transmitted between TOE components	Overwrite memory with zero three times	Immediately after use

[Table 6-7] Cryptographic Key Destruction Timing and Event

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation, or
FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [the 'Purpose' column in [Table 6-8]] in accordance with a specified cryptographic algorithm [the 'Algorithm' column in [Table 6-8]] and cryptographic key sizes [the 'Key Size' column in [Table 6-8]] that meet the following: [the 'Standard' column in [Table 6-8]].

Standard	Algorithm	Key Size	Purpose
ISO/IEC 29167-10:2017	AES-128-CBC	128-bit	Encryption/decryption of the stored data encryption key using a KEK
			Encryption/decryption of phone numbers and email addresses
			Encryption/decryption for delivering authentication elements and the server/user authentication information generation key to

			AutoPassword Enterprise v4 Android/iOS App
			Encryption/decryption when storing the server/user authentication information generation key
			Encryption/decryption of the private key password
			Encryption/decryption of DBMS connection information
			Encryption/decryption of the SMTP password
ISO/IEC 9797-2	HMAC-SHA256	256-bit	Mutual verification during communication with the AutoPassword Enterprise v4 Android/iOS App
			Generation of server/user authentication information
RFC 3447	RSA 2048	2048-bit	Digital signature generation and verification for the AutoPassword Enterprise v4 Android/iOS App
			Encryption/decryption of the secret key provided to the business server
			Server verification in TLS 1.2
RFC 5289	AES256-GCM	256-bit	TLS 1.2 communication encryption
ISO/IEC 10118-3:2004	SHA256	256-bit	Hashing passwords for storage
			TOE integrity verification
	SHA384	384-bit	Integrity check for data communicated between TOE components

[Table 6-8] Cryptographic Operation

FCS_RBG.1 Random bit generation (RBG)

Hierarchical to: No other components.

Dependencies: [FCS_RBG.2 Random bit generation (external seeding), or
FCS_RBG.3 Random bit generation (internal seeding – single source)]
FPT_FLS.1 Failure with preservation of secure state
FPT_TST.1 TSF self-testing

FCS_RBG.1.1 The TSF shall perform deterministic random bit generation services using [HASH_DRBG (SHA512)] in accordance with [NIST SP 800-90A Rev.1] after initialization.

FCS_RBG.1.2 The TSF shall use a *TSF interface for obtaining entropy* for initialization and reseeding.

FCS_RBG.1.3 The TSF shall update the DRBG state by *reseeding* using a *TSF interface for obtaining entropy [getrandom()]* in the following situations:

- *on the condition: [after 256 generations, 1 hour after seeding, or upon error occurrence]*

in accordance with [NIST SP 800-90A Rev. 1].

FCS_RBG.3 Random bit generation (internal seeding – single source)

Hierarchical to: No other components.
Dependencies: FCS_RBG.1 Random bit generation (RBG)

FCS_RBG.3.1 The TSF shall be able to seed the DRBG using a *TSF software-based entropy source* [getrandom()] with [256] bits of min-entropy.

FCS_RBG.5 Random bit generation (combining entropy sources)

Hierarchical to: No other components.
Dependencies: FCS_RBG.1 Random bit generation (RBG)
[FCS_RBG.2 Random bit generation (external seeding), or
FCS_RBG.3 Random bit generation (internal seeding - single source), or FCS_RBG.4 Random bit generation (internal seeding – multiple sources)]

FCS_RBG.5.1 The TSF shall [perform a Hashing operation on the] *input from TSF interface(s) for obtaining entropy* resulting in a minimum of [256] bits of min-entropy to create the entropy input into the derivation function as defined in [NIST SP 800-90A Rev. 1].

6.1.3 Identification and authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *[5]* unsuccessful authentication attempts occur related to [administrator authentication attempts].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall [perform the following actions].

[

a) Display an authentication failure message on the authentication screen and block authentication for 5 minutes.

b) The authentication block is released after 5 minutes.

]

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [the following quality metric].

[

a) Length must be between 10 and 20 characters, inclusive.

b) Must include at least one character from each of the following groups: English uppercase and lowercase letters, numbers, and special characters (@, $, !, %, *, #, ?, &).

c) Prohibition of using 3 or more identical consecutive characters or numbers.

d) Prohibition of using 4 or more sequential characters or numbers from a keyboard layout.

e) Prohibition of using 4 or more sequential numbers.

f) Prohibition of using 4 or more sequential alphabetic characters.

]

FIA_SOS.2 TSF Generation of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.2.1 The TSF shall provide a mechanism to generate **server/user authentication information** that meet [the following quality metric].

Category	Server Authentication Information	User Authentication Information
Generation Entity	Generated separately by AutoPassword Enterprise v4 Server and AutoPassword Enterprise v4 Android/iOS App	Generated separately by AutoPassword Enterprise v4 Server and AutoPassword Enterprise v4 Android/iOS App
Components	• Session ID of the client accessing the business server • Generation time • Generation key for server/user authentication information • Digital signature verification data	• IP address of the AutoPassword Enterprise v4 Android/iOS App • Session ID of the client accessing the business server • Current time • Generation key for server/user authentication information • Digital signature verification data
Cryptographic Algorithm	• HMAC-SHA-256 • AES-128-CBC	• HMAC-SHA-256 • AES-128-CBC • RSA2048 • SHA-256

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF-generated **server/user authentication information** for [server authentication and user authentication].

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4 Single-use authentication mechanisms

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [the following authentication mechanisms].

Authentication Type	Authentication Mechanism
Administrator Authentication	Ensures the uniqueness of a Random Value for each session.
Server Authentication	Ensures the uniqueness of a Random Value for each session.
User Authentication	Ensures the uniqueness of a Random Value for each session.

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [the following feedback] to the user while the authentication is in progress.

[

a) A character (●) to replace the input password.

b) Provision of only the failure result upon authentication failure, excluding the cause.

]

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

6.1.4 Security management

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to ***perform management actions*** of the functions [listed below] to [the authorized administrator].

Category	Function
Identification and Authentication	Register and modify administrator accounts
	Register, delete, and modify user accounts
	Register and delete authenticators for each user
	Register, delete, and modify integrated services
	Issue and renew integrated service keys
Secure Session Management	Resetting the user authentication failure count
	Unlocking user sessions
Audit Record	Viewing audit records
Security Management	Configuring allowed IP addresses for web management console access
	Configuring credentials for accessing external IT entities
Self-Protection	Performing an integrity check of TOE settings and the TOE itself at the administrator's request

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MTD.1.1 The TSF shall restrict the ability to *[manage]* the [following TSF data] to [the authorized administrator].

[

a) Administrator identification and authentication data

b) User identification and authentication data

c) Integrated service identification and authentication data

d) Authentication logs

e) Audit logs

f) Email address for alarm notifications

g) SMTP server information

h) Integrity verification results

]

FMT_PWD.1 Management of ID and password (Extended)

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_PWD.1.1 The TSF shall restrict the ability to manage the password of [none] to [none].

1. [None]
2. [None]

FMT_PWD.1.2 The TSF shall restrict the ability to manage the ID of [none] to [none].

1. [None]
2. [None]

FMT_PWD.1.3 The TSF shall provide the capability for *setting ID and password when installing*.

FMT_SMF.1 Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

[

a) The list of security functions specified in FMT_MOF.1

b) The list of TSF data management specified in FMT_MTD.1

c) The list of ID and password management specified in FMT_PWD.1

]

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [the following administrator roles].

[

a) Management of users and authenticators

b) Management of integrated services

c) Viewing of logs

d) Management of the administrator account

e) Management of settings

]

FMT_SMR.1.2 The TSF shall be able to associate users with **the roles defined in FMT_SMR.1.1**.

6.1.5 Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [failure in server authentication information generation, failure in user authentication information generation].

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_ITT.1.1 The TSF shall protect TSF data from *disclosure, modification* when it is transmitted between separate parts of the TOE.

FPT_PST.1 Basic protection of stored TSF data (Extended)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_PST.1.1 The TSF shall protect [the following TSF data] stored in containers controlled by the TSF from the unauthorized *disclosure, modification*.

[

a) Cryptographic keys (Asymmetric key for server authentication in TLS 1.2, Asymmetric key for verifying user authentication information from the App, Stored data encryption key, Encryption key for data transmitted between the Server and the business server, Encryption key for data transmitted between TOE components, and the Generation key for server/user authentication information)

b) TOE settings stored in the DBMS

c) Private key password

d) SMTP password

e) DBMS connection information

f) Administrator password

g) Audit data

]

FPT_TST.1 TSF self-testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1 The TSF shall run a suite of the following self-tests *during initial start-up, periodically during normal operation* to demonstrate the correct operation of *the TSF*:

[

- The baseline service first verifies the normal operation of other services.
- The baseline service performs a self-test by checking the normal operation of the authentication information generation function.

]

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of *TSF data*.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of *the TSF*.

6.1.6 TOE access

FTA_MCS.2 Per user attribute limitation on multiple concurrent sessions

Hierarchical to: FTA_MCS.1 Basic limitation on multiple concurrent sessions
Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same **administrator** according to the rules [the maximum number of concurrent sessions for the same administrator is restricted to one].

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of [1] sessions per user.

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [10-minute period of **administrator** inactivity].

FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny **administrative access** session establishment based on [the accessing IP address].

6.2 Assurance requirements

The assurance requirements of this Security Target are composed of the assurance components from Part 5 of the Common Criteria (CC:2022 R1), and the assurance level is EAL1. The following presents the assurance components for these assurance requirements.

Assurance class	Assurance components	
ST evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functional specification
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing - conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

6.2.1 ST evaluation

ASE_INT.1 ST introduction

Dependencies

No dependencies.

Developer action elements

ASE_INT.1.1D

The developer shall provide an ST introduction.

Content and presentation elements

ASE_INT.1.1C

The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C

The ST reference shall uniquely identify the ST.

ASE_INT.1.3C

The TOE reference shall uniquely identify the TOE.

ASE_INT.1.4C

The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C

The TOE overview shall identify the TOE type.

ASE_INT.1.6C

The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C

For a multi-assurance ST, the TOE overview shall describe the TSF organization in terms of the sub-TSFs defined in the PP-Configuration the ST claims conformance to.

ASE_INT.1.8C

The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.9C

The TOE description shall describe the logical scope of the TOE.

Evaluator action elements

ASE_INT.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E

The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies

ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Direct rationale stated security requirements

Developer action elements

ASE_CCL.1.1D

The developer shall provide a conformance claim.

ASE_CCL.1.2D

The developer shall provide a conformance claim rationale.

Content and presentation elements

ASE_CCL.1.1C

The conformance claim shall identify the edition of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C

The conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C

The conformance claim shall describe the conformance of the ST as either "CC Part 3 conformant" or "CC Part 3 extended".

ASE_CCL.1.4C

The conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C

The conformance claim shall identify a PP-Configuration, or all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C

The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C

The conformance claim shall describe any conformance of the ST to a PP as PP-Conformant.

ASE_CCL.1.8C

The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PP-Configuration or PPs for which conformance is being claimed.

ASE_CCL.1.9C

The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PP-Configuration, PPs and any functional packages for which conformance is being claimed.

ASE_CCL.1.10C

The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PP-Configuration, PPs, and any functional package for which conformance is being claimed.

ASE_CCL.1.11C

The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PP-Configuration, PPs, and any functional packages for which conformance is being claimed.

ASE_CCL.1.12C

The conformance claim for PP(s) or a PP-Configuration shall be exact, strict, or demonstrable or a list of conformance types.

ASE_CCL.1.13C

If the conformance claim identifies a set of Evaluation methods and Evaluation activities derived from CEM work units that shall be used to evaluate the TOE then this set shall include all those that are included in any package, PP, or PP-Module in a PP-Configuration to which the ST claims conformance, and no others.

Evaluator action elements

ASE_CCL.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 Security problem definition

Dependencies

No dependencies.

Developer action elements

ASE_SPD.1.1D

The developer shall provide a security problem definition.

Content and presentation elements

ASE_SPD.1.1C

The security problem definition shall describe the threats.

ASE_SPD.1.2C

All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C

The security problem definition shall describe the OSPs.

ASE_SPD.1.4C

The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements

ASE_SPD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.1 Security objectives for the operational environment

Dependencies

No dependencies.

Developer action elements

ASE_OBJ.1.1D

The developer shall provide a statement of security objectives for the operational environment.

ASE_OBJ.1.2D

The developer shall provide a security objectives rationale for the operational environment.

Content and presentation elements

ASE_OBJ.1.1C

The statement of security objectives shall describe the security objectives for the operational environment.

ASE_OBJ.1.2C

The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.1.3C

The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements

ASE_OBJ.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies

No dependencies.

Developer action elements

ASE_ECD.1.1D

The developer shall provide a statement of security requirements.

ASE_ECD.1.2D

The developer shall provide an extended components definition.

Content and presentation elements

ASE_ECD.1.1C

The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C

The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C

The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C

The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C

The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements may be demonstrated.

Evaluator action elements

ASE_ECD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E

The evaluator shall confirm that no extended component may be clearly expressed using existing components.

ASE_REQ.1 Direct rationale security requirements

Dependencies

ASE_ECD.1 Extended components definition

ASE_SPD.1 Security problem definition

ASE_OBJ.1 Security objectives for the operational environment

Developer action elements

ASE_REQ.1.1D

The developer shall provide a statement of security requirements.

ASE_REQ.1.2D

The developer shall provide a security requirements rationale.

Content and presentation elements

ASE_REQ.1.1C

The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C

For a single-assurance ST, the statement of security requirements shall define the global set of SARs that apply to the entire TOE. The sets of SARs shall be consistent with the PPs or PP-Configuration to which the ST claims conformance.

ASE_REQ.1.3C

For a multi-assurance ST, the statement of security requirements shall define the global set of SARs that apply to the entire TOE and the sets of SARs that apply to each sub-TSF. The sets of SARs shall be consistent with the multi-assurance PP-Configuration to which the ST claims conformance.

ASE_REQ.1.4C

All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.5C

The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.6C

All operations shall be performed correctly.

ASE_REQ.1.7C

Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.8C

The security requirements rationale shall trace each SFR back to the threats countered by that SFR and the OSPs enforced by that SFR.

The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) counter all threats for the TOE.

ASE_REQ.1.9C

The security requirements rationale shall demonstrate that the SFRs (in conjunction with the security objectives for the environment) enforce all OSPs.

ASE_REQ.1.10C

The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.1.11C

The statement of security requirements shall be internally consistent.

ASE_REQ.1.12C

If the ST defines sets of SARs that expand the sets of SARs of the PPs or PP-Configuration it claims conformance to, the security requirements rationale shall include an assurance rationale that justifies the consistency of the extension and provides a rationale for the disposition of any Evaluation methods and Evaluation activities identified in the conformance statement that are affected by the extension of the sets of SARs

Evaluator action elements

ASE_REQ.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 Security problem definition

Dependencies

No dependencies.

Developer action elements

ASE_SPD.1.1D

The developer shall provide a security problem definition.

Content and presentation elements

ASE_SPD.1.1C

The security problem definition shall describe the threats.

ASE_SPD.1.2C

All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C

The security problem definition shall describe the OSPs.

ASE_SPD.1.4C

The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements

ASE_SPD.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies

ASE_INT.1 ST introduction

ASE_REQ.1 Direct rationale stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements

ASE_TSS.1.1D

The developer shall provide a TOE summary specification.

Content and presentation elements

ASE_TSS.1.1C

The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements

ASE_TSS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E

The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.2 Development

ADV_FSP.1 Basic functional specification

Dependencies

No dependencies.

Developer action elements

ADV_FSP.1.1D

The developer shall provide a functional specification.

ADV_FSP.1.2D

The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements

ADV_FSP.1.1C

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements

ADV_FSP.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

6.2.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies

ADV_FSP.1 Basic functional specification

Developer action elements

AGD_OPE.1.1D

The developer shall provide operational user guidance.

Content and presentation elements

AGD_OPE.1.1C

The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C

The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C

The operational user guidance shall, for each user role, describe the security controls to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C

The operational user guidance shall be clear and reasonable.

Evaluator action elements

AGD_OPE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1 Preparative procedures

Dependencies

No dependencies.

Developer action elements

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

Content and presentation elements

AGD_PRE.1.1C

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements

AGD_PRE.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.2.4 Life-cycle support

ALC_CMC.1 Labelling of the TOE

Dependencies

ALC_CMS.1 TOE CM coverage

Developer action elements

ALC_CMC.1.1D

The developer shall provide the TOE and a unique reference for the TOE.

Content and presentation elements

ALC_CMC.1.1C

The TOE shall be labelled with its unique reference.

Evaluator action elements

ALC_CMC.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.1 TOE CM coverage

Dependencies

No dependencies.

Developer action elements

ALC_CMS.1.1D

The developer shall provide a configuration list for the TOE.

Content and presentation elements

ALC_CMS.1.1C

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C

The configuration list shall uniquely identify the configuration items.

Evaluator action elements

ALC_CMS.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.5 Tests

ATE_IND.1 Independent testing - conformance

Dependencies

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements

ATE_IND.1.1D

The developer shall provide the TOE for testing.

Content and presentation elements

ATE_IND.1.1C

The TOE shall be suitable for testing.

Evaluator action elements

ATE_IND.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2E

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability assessment

AVA_VAN.1 Vulnerability survey

Dependencies

ADV_FSP.1 Basic functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements

AVA_VAN.1.1D

The developer shall provide the TOE for testing.

Content and presentation elements

AVA_VAN.1.1C

The TOE shall be suitable for testing.

Evaluator action elements

AVA_VAN.1.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2E

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6.3 Dependency rationale

6.3.1 TOE security functional requirements dependency

The following [Table 6-9] shows the dependencies of the TOE's security functional components.

Rationale (1): FAU_GEN.1 has a dependency on FPT_STM.1. However, since the TOE uses a reliable timestamp provided by the TOE operational environment to accurately record security-related events, this dependency is satisfied by the security objective for the operational environment, OE.TIMESTAMP, instead of FPT_STM.1.

Rationale (2): In addition to FAU_GEN.1, FAU_STG.1 has a dependency on FTP_ITC.1. However, since the TOE stores audit records in a physically secure DBMS provided by the TOE operational environment, this dependency is satisfied by the security objective for the operational environment, OE.DBMS, instead of FTP_ITC.1.

Rationale (3): FAU_STG.4 and FAU_STG.5 have a dependency on FAU_STG.2. However, since the TOE stores audit records in a physically secure DBMS provided by the TOE operational environment, this dependency is satisfied by the security objective for the operational environment, OE.DBMS, instead of FAU_STG.2.

The dependencies of FIA_AFL.1 and FIA_UAU.7 on FIA_UAU.1 are satisfied by FIA_UAU.2, which is hierarchical to FIA_UAU.1.

The dependencies of FIA_UAU.2, FMT_SMR.1, and FTA_MCS.2 on FIA_UID.1 are satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1.

No.	Security Functional Component	Dependency	Reference No.

1	FAU_ARP.1	FAU_SAA.1	3
2	FAU_GEN.1	FPT_STM.1	Rationale (1)
3	FAU_SAA.1	FAU_GEN.1	2
4	FAU_SAR.1	FAU_GEN.1	2
5	FAU_SAR.3	FAU_SAR.1	4
6	FAU_STG.1	FAU_GEN.1 FTP_ITC.1	2 Rationale (2)
7	FAU_STG.4	FAU_STG.2	Rationale (3)
8	FAU_STG.5	FAU_STG.2	Rationale (3)
9	FCS_CKM.1	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1] [FCS_RBG.1 or FCS_RNG.1] FCS_CKM.6	10, 11, 13 14 12
10	FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	9, 11
11	FCS_CKM.5	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.6	10, 13 12
12	FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	9, 11
13	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6	9, 11 12
14	FCS_RBG.1	[FCS_RBG.2 or FCS_RBG.3] FPT_FLS.1 FPT_TST.1	15 29 32
15	FCS_RBG.3	FCS_RBG.1	14
16	FCS_RBG.5	FCS_RBG.1 [FCS_RBG.2 or FCS_RBG.3 or FCS_RBG.4]	14 15
17	FIA_AFL.1	FIA_UAU.1	20
18	FIA_SOS.1	-	-
19	FIA_SOS.2	-	-
20	FIA_UAU.2	FIA_UID.1	23
21	FIA_UAU.4	-	-
22	FIA_UAU.7	FIA_UAU.1	20
23	FIA_UID.2	-	-
24	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	27 28
25	FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	27 28
26	FMT_PWD.1 (Extended)	FMT_SMF.1 FMT_SMR.1	27 28
27	FMT_SMF.1	-	-
28	FMT_SMR.1	FIA_UID.1	23
29	FPT_FLS.1	-	-

30	FPT_ITT.1	-	-
31	FPT_PST.1 (Extended)	-	-
32	FPT_TST.1	-	-
33	FTA_MCS.2	FIA_UID.1	23
34	FTA_SSL.3	FMT_SMR.1	28
35	FTA_TSE.1	-	-

[Table 6-9] TOE security functional component dependencies

6.3.2 TOE security assurance requirements dependency

The dependencies for each assurance package provided in the Common Criteria are already satisfied. Therefore, the rationale is omitted here.

6.4 Security requirements rationale

6.4.1 Rationale for the security functional requirements

The rationale for the security functional requirements demonstrates the following: each threat and organizational security policy is addressed by at least one security functional requirement. Each security functional requirement traces back to at least one threat or organizational security policy.

Security functional requirement	T. SESSION_HIJACK	T. RETRY_AUTH_ATTEMPT	T. IMPERSONATION	T. REPLAY	T. WEAK_PASSWORD	T. UNAUTHORIZED_INFO_LEAK	T. STORED_DATA_LEAKAGE	T. TRANSMISSION_DATA_DAMAGE	T. WEAK_CRYPTO_PROTOCOLS	T. TSF_COMPROMISE	P. AUDIT	P. SECURE_OPERATION	P. CRYPTO_STRENGTH
FAU_ARP.1										O			
FAU_GEN.1											O		
FAU_SAA.1										O			
FAU_SAR.1											O		
FAU_SAR.3											O		
FAU_STG.1											O		
FAU_STG.4											O		
FAU_STG.5											O		
FCS_CKM.1						O	O	O	O				O
FCS_CKM.2						O	O	O	O				O
FCS_CKM.5						O	O	O	O				O
FCS_CKM.6						O	O	O	O				O

FCS_COP.1						O	O	O	O				O
FCS_RBG.1						O	O	O	O				O
FCS_RBG.3						O	O	O	O				O
FCS_RBG.5						O	O	O	O				O
FIA_AFL.1		O	O							O			
FIA_SOS.1					O								
FIA_SOS.2			O	O									
FIA_UAU.2			O							O			
FIA_UAU.4			O	O						O			
FIA_UAU.7			O		O					O			
FIA_UID.2			O							O			
FMT_MOF.1										O		O	
FMT_MTD.1										O		O	
FMT_PWD.1					O					O		O	
FMT_SMF.1										O		O	
FMT_SMR.1										O		O	
FPT_FLS.1						O	O	O	O				O
FPT_ITT.1								O					
FPT_PST.1							O						
FPT_TST.1						O	O	O	O	O			O
FTA_MCS.2	O												
FTA_SSL.3	O												
FTA_TSE.1	O												

T.SESSION_HIJACK	FTA_MCS.2, FTA_SSL.3, FTA_TSE.1
FTA_MCS.2 counters T.SESSION_HIJACK by restricting duplicate access to the TOE with the same user account or identical privileges. FTA_SSL.3 counters T.SESSION_HIJACK by ensuring session lock or termination for an interactive session after a period of user inactivity. FTA_TSE.1 counters T.SESSION_HIJACK by ensuring that the establishment of an authorized user access session is determined based on attributes such as IP address.	

T.RETRY_AUTH_ATTEMPT	FIA_AFL.1
FIA_AFL.1 counters T.RETRY_AUTH_ATTEMPT by defining the number of failed authentication attempts for an administrator and ensuring that a responsive action is taken when the defined number is met.	

T.IMPERSONATION	FIA_AFL.1, FIA_SOS.2, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2
FIA_AFL.1 counters T.IMPERSONATION by defining the number of failed authentication attempts for an administrator and ensuring a responsive action is taken when the defined number is met. FIA_SOS.2, FIA_UAU.2, and FIA_UAU.4 counter T.IMPERSONATION by ensuring that a user attempting to access the TOE is successfully authenticated. FIA_UAU.7 counters T.IMPERSONATION by ensuring that only masked values are displayed or nothing is displayed to the user during authentication, and that no feedback on the reason for failure is provided upon authentication failure. FIA_UID.2 counters T.IMPERSONATION by ensuring that a user attempting to access the TOE is successfully identified.	

T.REPLAY	FIA_SOS.2, FIA_UAU.4
FIA_SOS.2 counters T.REPLAY by ensuring the prevention of server/user authentication information reuse during its generation. FIA_UAU.4 counters T.REPLAY by ensuring the ability to prevent the reuse of authentication data.	

T.WEAK_PASSWORD	FIA_SOS.1, FIA_UAU.7, FMT_PWD.1
FIA_SOS.1 counters T.WEAK_PASSWORD by verifying that passwords meet the complexity rules. FIA_UAU.7 counters T.WEAK_PASSWORD by ensuring that only masked values are displayed or nothing is displayed to the user during authentication. FMT_PWD.1 counters T.WEAK_PASSWORD by providing the functionality to set an ID and password during the installation process.	

T.UNAUTHORIZED_INFO_LEAK	FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5, FPT_FLS.1, FPT_TST.1
FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5, FPT_FLS.1, and FPT_TST.1 counter T.UNAUTHORIZED_INFO_LEAK by ensuring that cryptographic keys are generated and distributed according to secure cryptographic algorithms and key sizes when encrypting/decrypting critical user information stored in the database. FCS_CKM.6 counters T.UNAUTHORIZED_INFO_LEAK by ensuring that after the encryption/decryption of critical user information stored in the database, the cryptographic keys and related information are destroyed according to the specified key destruction method.	

FCS_COP.1 counters T.UNAUTHORIZED_INFO_LEAK by ensuring that cryptographic operations are performed according to the specified secure algorithms and key sizes when encrypting/decrypting critical user information stored in the database.

T.STORED_DATA_LEAKAGE	FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5, FPT_FLS.1, FPT_PST.1, FPT_TST.1
FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5, FPT_FLS.1, and FPT_TST.1 counter T.STORED_DATA_LEAKAGE by ensuring that cryptographic keys are generated and distributed according to secure cryptographic algorithms and key sizes for stored data encryption. FCS_CKM.6 counters T.STORED_DATA_LEAKAGE by ensuring that upon completion of stored data encryption, the cryptographic keys and related information are destroyed according to the specified key destruction method. FCS_COP.1 counters T.STORED_DATA_LEAKAGE by ensuring that cryptographic operations for stored data encryption are performed according to the specified secure algorithms and key sizes. FPT_PST.1 counters T.STORED_DATA_LEAKAGE by ensuring that stored TSF data is protected from leakage threats through methods such as encryption and access control.	

T.TRANSMISSION_DATA_DAMAGE	FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5, FPT_FLS.1, FPT_ITT.1, FPT_TST.1
FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5, FPT_FLS.1, and FPT_TST.1 counter T.TRANSMISSION_DATA_DAMAGE by ensuring that cryptographic keys are generated and distributed according to secure cryptographic algorithms and key sizes for encrypted communication. FCS_CKM.6 counters T.TRANSMISSION_DATA_DAMAGE by ensuring that upon termination of encrypted communication, the cryptographic keys and related information are destroyed according to the specified key destruction method. FCS_COP.1 counters T.TRANSMISSION_DATA_DAMAGE by ensuring that cryptographic operations for encrypted communication are performed according to the specified secure algorithms and key sizes. FPT_ITT.1 counters T.TRANSMISSION_DATA_DAMAGE by ensuring the confidentiality and integrity of data transmitted between TOE components.	

T.WEAK_CRYPTO_PROTOCOLS	FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5, FPT_FLS.1, FPT_TST.1

FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5, FPT_FLS.1, and FPT_TST.1 counter T.WEAK_CRYPTO_PROTOCOLS by ensuring that for transmitted data encryption, cryptographic keys are generated and distributed according to the algorithms and key lengths required by standard cryptographic algorithms with a security strength of 112 bits or higher.

FCS_CKM.6 counters T.WEAK_CRYPTO_PROTOCOLS by ensuring that cryptographic keys and related information are destroyed according to the specified destruction method.

FCS_COP.1 counters T.WEAK_CRYPTO_PROTOCOLS by ensuring that cryptographic operations for transmitted data encryption are performed according to standard cryptographic algorithms and key lengths with a security strength of 112 bits or higher.

T.TSF_COMPROMISE	FAU_ARP.1, FAU_SAA.1, FIA_AFL.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2, FMT_MOF.1, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, FMT_SMR.1, FPT_TST.1

FAU_ARP.1 counters T.TSF_COMPROMISE by ensuring the ability to take responsive action when a security violation, such as a TOE integrity compromise, is detected.

FAU_SAA.1 counters T.TSF_COMPROMISE by ensuring the ability to analyze audited events to indicate security violations, such as a TOE integrity compromise.

FIA_AFL.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, and FIA_UID.2 counter T.TSF_COMPROMISE by ensuring that access to the TOE is only possible after successful user identification and authentication, thereby blocking bypass attempts from threat agents.

FMT_MOF.1, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, and FMT_SMR.1 counter T.TSF_COMPROMISE by restricting access to and configuration of management functions to authorized administrators, providing security policies and functions only to them and thereby blocking unauthorized access from threat agents.

FPT_TST.1 counters T.TSF_COMPROMISE by ensuring TSF self-testing for the correct operation of the TOE and providing authorized administrators with the ability to verify the integrity of TSF data and the TSF.

P.AUDIT	FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.4, FAU_STG.5

FAU_GEN.1 satisfies P.AUDIT by ensuring that audit records are generated for auditable events such as the start-up/shutdown of audit functions and the success/failure of administrator identification and authentication.

FAU_SAR.1 satisfies P.AUDIT by providing authorized administrators with the capability to view audit records and ensuring that the records are provided in a manner suitable for interpretation.

FAU_SAR.3 satisfies P.AUDIT by providing a selective audit review function based on criteria with logical relations for audit data.

FAU_STG.1 satisfies P.AUDIT by providing the capability for the TOE server to store audit data in a local repository or transmit it in real-time to an external IT entity for storage using a secure channel.

FAU_STG.4 satisfies P.AUDIT by ensuring that appropriate actions are taken when the TOE server's audit trail exceeds its storage threshold.

FAU_STG.5 satisfies P.AUDIT by ensuring the ability to take appropriate action when the TOE server's audit trail is full.

P.SECURE_OPERATION	FMT_MOF.1, FMT_MTD.1, FMT_PWD.1, FMT_SMF.1, FMT_SMR.1

FMT_MOF.1 satisfies P.SECURE_OPERATION by ensuring that only authorized administrators have the ability to manage security functions.

FMT_MTD.1 satisfies P.SECURE_OPERATION by ensuring that only authorized administrators have the ability to manage TSF data.

FMT_PWD.1 satisfies P.SECURE_OPERATION by providing the functionality to set an ID and password during the installation process.

FMT_SMF.1 satisfies P.SECURE_OPERATION by requiring the specification of management functions that the TSF must perform, such as for security functions, security attributes, and TSF data.

FMT_SMR.1 satisfies P.SECURE_OPERATION by ensuring the specification of authorized roles related to security management.

P.CRYPTO_STRENGTH	FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5, FPT_FLS.1, FPT_TST.1

FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5, FPT_FLS.1, and FPT_TST.1 satisfy P.CRYPTO_STRENGTH by ensuring that for data encryption, the necessary cryptographic keys are securely generated and distributed according to standard cryptographic algorithms with a security strength of 112 bits or higher.

FCS_COP.1 satisfies P.CRYPTO_STRENGTH by ensuring that data encryption is performed according to standard cryptographic algorithms and key lengths with a security strength of 112 bits or higher.

7 TOE summary specification

7.1 Security audit

7.1.1 Audit record generation

When an auditable event as listed below occurs, the TOE records an audit record that includes the date and time of the event, type of event, subject identity, outcome of the event, and other audit-relevant information. When generating audit data, the TOE associates the identity of the user who caused the event with the auditable event by including the user's identity in the audit record.

Security Functional Component	Auditable Event	Additional Audit Record Contents
FAU_ARP.1	Actions taken due to potential security violations	
FAU_GEN.1	None	
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms	
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.3	The parameters used for the viewing	
FAU_STG.1	None	
FAU_STG.4	Actions taken due to exceeding of a threshold	
FAU_STG.5	Actions taken due to the audit data storage failure	
FCS_CKM.1	Success and failure of the activity	
FCS_CKM.2	Success and failure of the activity	
FCS_CKM.5	Success and failure of the activity	
FCS_CKM.6	Success and failure of the activity	
FCS_COP.1	Success and failure, and the type of cryptographic operation	
FCS_RBG.1	Failure of the randomization process, failure to initialize or reseed	
FCS_RBG.3	None	
FCS_RBG.5	None	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.	
FIA_SOS.1	Rejection by the TSF of any tested secret	
FIA_SOS.2	Rejection by the TSF of any tested secret	

FIA_UAU.2	Unsuccessful use of the authentication mechanism	
FIA_UAU.4	Attempts to reuse authentication data	
FIA_UAU.7	None	
FIA_UID.2	Unsuccessful use of the user identification mechanism, including the user identity provided	
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF	
FMT_MTD.1	All modifications to the values of TSF data	Modified TSF data value
FMT_PWD.1	All modifications to the password	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modifications to the group of users that are part of a role	
FPT_FLS.1	Failure of the TSF	
FPT_ITT.1	None	
FPT_PST.1	None	
FPT_TST.1	Execution of the TSF self-tests and the results of the tests	Modified TSF data or executable code in case of integrity violation
FTA_MCS.2	Rejection of a new session based on the limitation of multiple concurrent sessions	
FTA_SSL.3	Termination of an interactive session by the session locking mechanism	
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	

Related SFR FAU_GEN.1

7.1.2 Audit record storage and viewing

Audit records generated by the TOE are stored in a DBMS, and only authorized administrators can view them. The TOE provides a function to search audit records using full AND or full OR conditions. It also provides the capability to sort and view the records in ascending and descending order by type, code, event name, and date.

Related SFR FAU_SAR.1, FAU_SAR.3, FAU_STG.1

7.1.3 Potential violation analysis

When the TOE detects a potential security violation among the audited events, it sends a potential violation alarm email to the email address registered by the authorized administrator. Potential security violations include: authentication failure audit events; self-test failures and integrity violations among auditable events; and the sending of alarm emails related to the prediction and prevention of audit record loss.

Related SFR FAU_ARP.1, FAU_SAA.1

7.1.4 Actions on predicted audit record loss and prevention of loss

When the audit record storage, allocated for 10,000 events, exceeds the specified thresholds of 60%, 70%, and 80%, the TOE sends an alarm email once for each threshold range to the email address registered via the web management console. If the audit record storage becomes full, the oldest audit records are overwritten, and an alarm email is sent to the email address registered by the authorized administrator.

Related SFR FAU_STG.4, FAU_STG.5

7.2 Cryptographic support

7.2.1 Cryptographic key management and operation

The TOE generates the random bits necessary to create secure cryptographic keys and uses various cryptographic functions to ensure data confidentiality and integrity. These functions are securely managed throughout the entire lifecycle of a cryptographic key, from generation, distribution, and derivation to use and destruction.

The TOE manages cryptographic keys and performs cryptographic operations according to the following standards and purposes.

Category	Standard	Algorithm	Key Size	Purpose
Cryptographic key generation	ISO/IEC 18033-2-2226	RSA 2048	2048-bit	Asymmetric key for server authentication during TLS 1.2 communication
				Asymmetric key to verify user authentication information from the AutoPassword Enterprise v4 Android/iOS App

	ISO/IEC 18033-2:2006	ECDHE	256-bit	Asymmetric key for session key generation during TLS 1.2 communication
	NIST SP 800-90A Rev.1	HASH_DRBG (SHA512)	128-bit	Stored data encryption key
				Encryption key for data transmitted between the AutoPassword Enterprise v4 Server and the business server
				Encryption key for data transmitted between TOE components
			160-bit	Generation key for server/user authentication information

Category	Standard	Distribution Method	Purpose
Cryptographic key distribution	ISO/IEC 18033-2:2006	ECDHE	Session key distribution for TLS 1.2 communication
	ISO/IEC 18033-2-2226	RSA 2048	Distribution of the encryption key for data transmitted between the AutoPassword Enterprise v4 Server and the business server
			Distribution of the encryption key for data transmitted between TOE components

Category	Standard	Key Derivation Algorithm	Key Size	Input Parameters	Key Type	Purpose
Cryptographic key derivation	TTAK.KO-12.0334	PBKDF2 (SHA512)	128-bit	KEK password input by user	AES_128	KEK derivation for TOE components
				Salt(128-bit)		
	ISO/IEC 11770-3	KDF	256-bit	Client random	AES_256	Session key derivation
				Server random		
				Shared secret		

Category	Cryptographic Key	Destruction Method	Point of Destruction
Cryptographic key destruction	Stored data encryption key	Overwrite memory with zero three times	Upon process termination
	KEK (Key Encryption Key)	Overwrite memory with zero three times	Immediately after use
	Key used during TLS 1.2 communication (Session key)	Overwrite memory with zero one time	Upon session termination

	Key used during TLS 1.2 communication (Shared secret, secp256r1 asymmetric key, RSA2048 asymmetric key)	Overwrite memory with zero one time	After TLS 1.2 handshake completion
	Encryption key for data transmitted between the AutoPassword Enterprise v4 Server and the business server	Overwrite memory with zero three times	Immediately after use
	Encryption key for data transmitted between TOE components	Overwrite memory with zero three times	Immediately after use

Category	Standard	Algorithm	Key Size	Purpose
Cryptographic operation	ISO/IEC 29167-10:2017	AES-128-CBC	128-bit	Encryption/decryption of the stored data encryption key using a KEK
				Encryption/decryption of phone numbers and email addresses
				Encryption/decryption for delivering authentication elements and the server/user authentication information generation key to AutoPassword Enterprise v4 Android/iOS App
				Encryption/decryption when storing the server/user authentication information generation key
				Encryption/decryption of the private key password
				Encryption/decryption of DBMS connection information
				Encryption/decryption of the SMTP password
	ISO/IEC 9797-2	HMAC-SHA256	256-bit	Mutual verification during communication with the AutoPassword Enterprise v4 Android/iOS App
				Generation of server/user authentication information

	RFC 3447	RSA 2048	2048-bit	Digital signature generation and verification for the AutoPassword Enterprise v4 Android/iOS App
				Encryption/decryption of the secret key provided to the business server
				Server verification in TLS 1.2
	RFC 5289	AES256-GCM	256-bit	TLS 1.2 communication encryption
	ISO/IEC 10118-3:2004	SHA256	256-bit	Hashing passwords for storage
				TOE integrity verification
		SHA384	384-bit	Integrity check for data communicated between TOE components

For its reliable security functions, the TOE provides a Deterministic Random Bit Generator (DRBG) that complies with the NIST SP 800-90A Rev.1 standard. Its main features are as follows.

Deterministic Random Bit Generation (DRBG)

- Algorithm: After initialization, the TSF performs a deterministic random bit generation service using the HASH_DRBG (SHA512) algorithm.
- Compliance standard: All random number generation procedures follow NIST SP 800-90A Rev.1.

Entropy source and seeding

- Entropy source: Unpredictability is ensured by using the getrandom() interface, a software-based entropy source within the TSF.
- Min-entropy: At least 256 bits of min-entropy are secured for the initial seeding of the DRBG.
- Entropy combination: A Hashing operation is performed on the input from the entropy source to combine the values, generating an entropy input of at least 256 bits for the derivation function in NIST SP 800-90A Rev.1.

Reseeding and state update

- To maintain the unpredictable security strength of the DRBG, the state is updated (reseeded) by obtaining new entropy through getrandom() when the specific conditions below are met.
- Reseeding conditions:
  - After 256 random numbers have been generated
  - When 1 hour has passed since the previous seeding (or reseeding)
  - When an error occurs during the random number generation process

Related SFR FCS_CKM.1, FCS_CKM.2, FCS_CKM.5, FCS_CKM.6, FCS_COP.1, FCS_RBG.1, FCS_RBG.3, FCS_RBG.5

7.3 Identification and authentication

7.3.1 Identification and authentication

Before any security functions are permitted, the TOE performs user authentication and identification based on an ID and password, and it detects failed authentication attempts. If the number of failed attempts reaches 5, authentication is blocked. If an administrator does not release the authentication block, it remains in effect for 5 minutes.

For both administrator and device administrator authentication, the uniqueness of a Random Value is ensured for each session to prevent the reuse of authentication data.

While authentication is in progress, a masking character (●) is displayed to the user in place of the entered password. Upon authentication failure, only the failure result is provided, excluding the cause.

Related SFR FIA_AFL.1, FIA_UAU.2, FIA_UAU.4, FIA_UAU.7, FIA_UID.2

7.3.2 Verification of secrets

Passwords are created according to the following rules:

- Length must be between 10 and 20 characters, inclusive.
- Must include at least one character from each of the following groups: English uppercase and lowercase letters, numbers, and special characters (@, $, !, %, *, #, ?, &).
- Prohibition of using 3 or more identical consecutive characters or numbers.
- Prohibition of using 4 or more sequential characters or numbers from a keyboard layout.
- Prohibition of using 4 or more sequential numbers.
- Prohibition of using 4 or more sequential alphabetic characters.

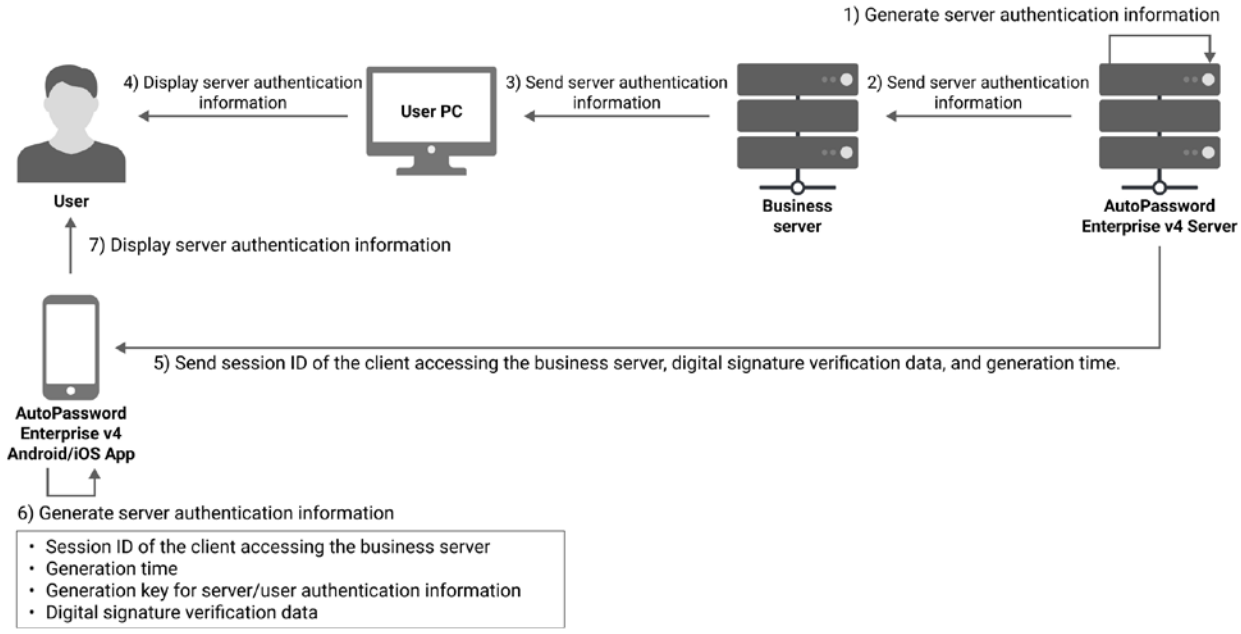
Related SFR FIA_SOS.1

7.3.3 Generation of secrets

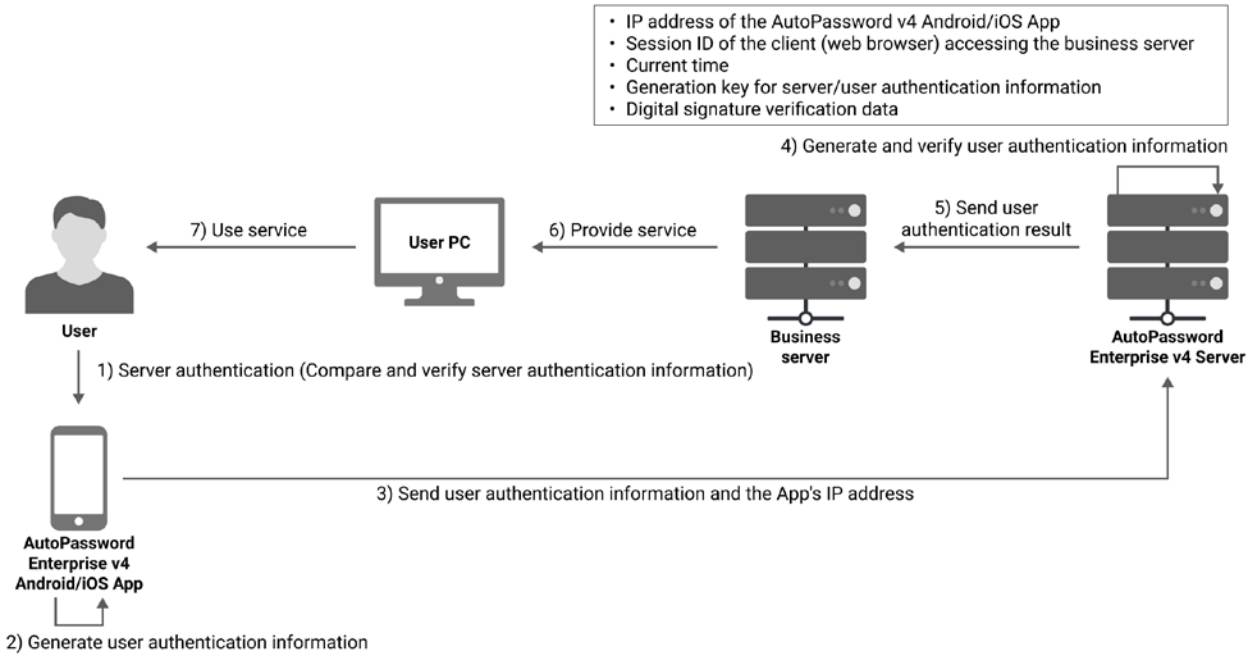
The AutoPassword Enterprise v4 Server and the AutoPassword Enterprise v4 Android/iOS App each generate server authentication information and user authentication information, respectively, using the following components and cryptographic algorithms. This information is used during server and user authentication.

Category	Server Authentication Information	User Authentication Information
Generation Entity	Generated separately by AutoPassword Enterprise v4 Server and AutoPassword Enterprise v4 Android/iOS App	Generated separately by AutoPassword Enterprise v4 Server and AutoPassword Enterprise v4 Android/iOS App
Components	• Session ID of the client accessing the business server • Generation time • Generation key for server/user authentication information • Digital signature verification data	• IP address of the AutoPassword Enterprise v4 Android/iOS App • Session ID of the client accessing the business server • Current time • Generation key for server/user authentication information • Digital signature verification data
Cryptographic Algorithm	• HMAC-SHA-256 • AES-128-CBC	• HMAC-SHA-256 • AES-128-CBC • RSA2048 • SHA-256

The flow for the generation and use of server authentication information is as follows.



The flow for the generation and use of user authentication information is as follows.



Related SFR FIA_SOS.2

7.4 Security management

7.4.1 General security management

During the installation process, the TOE provides a function to set the administrator's ID and password when accessed from an allowed IP address. Subsequently, it provides the authorized administrator with management capabilities for security functions and TSF data.

The main roles of the authorized administrator are as follows:

- Management of users and authenticators
- Management of integrated services
- Viewing of logs
- Management of the administrator account
- Management of settings

The ability to manage the following security functions is restricted to the authorized administrator.

Category	Function
Identification and Authentication	Register and modify administrator accounts
	Register, delete, and modify user accounts
	Register and delete authenticators for each user
	Register, delete, and modify integrated services
	Issue and renew integrated service keys
Secure Session Management	Resetting the user authentication failure count
	Unlocking user sessions
Audit Record	Viewing audit records
Security Management	Configuring allowed IP addresses for web management console access
	Configuring credentials for accessing external IT entities
Self-Protection	Performing an integrity check of TOE settings and the TOE itself at the administrator's request

The ability to manage the following TSF data is restricted to the authorized administrator:

- Administrator identification and authentication data
- User identification and authentication data
- Integrated service identification and authentication data
- Authentication logs
- Audit logs
- Email address for alarm notifications

- SMTP server information
- Integrity verification results

Related SFR FMT_MOF.1, FMT_MTD.1, FMT_PWD.1 (Extended), FMT_SMF.1, FMT_SMR.1

7.5 Protection of the TSF

7.5.1 Preserving a secure state during failures

Even if the generation of server authentication information or user authentication information fails, the TOE preserves a secure state in which its security functions are always performed.

Related SFR FPT_FLS.1

7.5.2 TSF data protection

When TSF data is transmitted between separate parts of the TOE, it must be protected from disclosure and modification using the TLS 1.2 protocol.

Among the TSF data, items such as cryptographic keys, TOE settings stored in the DBMS, the private key password, the SMTP password, DBMS connection information, and the administrator password are protected from unauthorized disclosure and modification by the following cryptographic algorithms.

TSF data to protect	Standard	Algorithm	Key Size
Cryptographic keys (Asymmetric key for server authentication in TLS 1.2, Asymmetric key for verifying user authentication information from the App, Stored data encryption key, Encryption key for data transmitted between the Server and the business server, Encryption key for data transmitted between TOE components, and the Generation key for server/user authentication information)	ISO/IEC 29167-10:2017	AES_128_CBC	128-bit
TOE settings stored in the DBMS			
Private key password			
SMTP password			
DBMS connection information			
Administrator password	ISO/IEC 10118-3:2004	SHA256	256-bit

Audit data is protected from unauthorized disclosure and modification by being stored in the DBMS.

Related SFR FPT_ITT.1, FPT_PST.1 (Extended)

7.5.3 Self-test and integrity verification

The AutoPassword Enterprise v4 Server runs self-tests to demonstrate the correct operation of the TSF during start-up and periodically during normal operation. The baseline service first verifies the normal operation of other services, after which the baseline service performs its self-test by checking whether the authentication information generation function is operating correctly.

The AutoPassword Enterprise v4 Android/iOS App runs self-tests to demonstrate the correct operation of the TSF during start-up (specifically, when the app restarts after being closed while connected to the server, and when it returns to the foreground after being in the background for over 20 seconds). The self-test checks whether the authentication information generation function is operating correctly.

The AutoPassword Enterprise v4 Server provides a function to verify the integrity of TSF data and the TSF itself during start-up, periodically during normal operation, and upon administrator request.

The AutoPassword Enterprise v4 Android/iOS App provides a function to verify the integrity of TSF data and the TSF itself during start-up (under the same conditions as the self-test).

Integrity is verified by comparing the hash values of key files such as configuration files, libraries, and executables. The SHA256 algorithm from the ISO/IEC 10118-3:2004 standard is used to generate these hash values.

If the self-test or integrity verification fails, the TOE terminates its own operation.

The targets for integrity verification for each TOE component are as follows.

AutoPassword Enterprise v4 Server

- /ESTAPP/autopassword/lib/*
- /ESTAPP/autopassword/bin/*
- /ESTAPP/autopassword/key/dek.enc
- /ESTAPP/autopassword/key/db.enc
- /ESTAPP/autopassword/key/ssl.enc
- /ESTAPP/autopassword/ssl/*
- /ESTAPP/autopassword/application/nginx/mobile/*
- /ESTAPP/autopassword/application/nginx/conf/nginx.conf

- /ESTAPP/autopassword/application/tomcat/webapps/*
- /ESTAPP/autopassword/application/tomcat/bin/setenv.sh
- /ESTAPP/autopassword/application/tomcat/bin/catalina.sh
- /ESTAPP/autopassword/application/tomcat/conf/server.xml
- /ESTAPP/autopassword/application/tomcat/conf/context.xml
- /ESTAPP/autopassword/application/tomcat/conf/logging.properties
- /ESTAPP/autopassword/application/tomcat/lib/ape_error.1.0.0.jar
- /ESTAPP/autopassword/application/tomcat/lib/keyManager.jar

AutoPassword Enterprise v4 Android App

- /lib/arm64-v8a/libotpandroid.so
- /keyData.dat
- /classes*.dex (e.g., classes.dex, classes1.dex, classes19.dex)

AutoPassword Enterprise v4 iOS App

- /AutoPasswordIDCard
- /Info.plist
- /InfoConfig.plist
- /KeyData.dat
- All library binaries and Info.plist files under the /Frameworks/ directory

Related SFR FPT_TST.1

7.6 TOE access

7.6.1 Session management

The TOE allows one session for an administrator to access the web management console.

Access to the web management console session is granted based on the connecting IP address, and the session is forcibly terminated after a 10-minute period of administrator inactivity.

Related SFR FTA_MCS.2, FTA_SSL.3, FTA_TSE.1