sallén

ZEN-D Security Target

Date: 2024-02-06

Created by jtsec BEYOND IT SECURITY CCGEN Create Common Criteria compliant documentation Simple and Easy

Change History

Version	Date	Author	Comment
0.1	2022/03/25	Gunnebo Security Group	First draft
0.2	2022/10/18	Gunnebo Security Group	Minor changes
0.3	2023/01/18	Gunnebo Security Group	Changes in sections 1.4, 3, 4. 6 and 7
0.4	2023/02/01	Gunnebo Security Group	Changes in sections 1.3, 1.4, 3,5, 4.2, 6 and 7
0.5	2023/02/24	Gunnebo Security Group	Addressed minor lab comments. Modified SPD, included P.ADMINS_AC. Removed USB assumption. Clarified Threat Agents
0.6	2023/03/11	Grupo Sallén Tech SLU	Developer updated by Grupo Sallén Tech SLU. Minor changes for consistency with functional tests
0.7	2023/07/28	Grupo Sallén Tech SLU	TOE version updated adding OpenVPN v2.4.4
0.8	2023/12/20	Grupo Sallén Tech SLU	Grupo Sallén Tech SLU
0.9	2024/02/06	Grupo Sallén Tech SLU	Physical scope updated

Table of contents

1 ST INTRODUCTION

1.1 ST REFERENCE

Title: ZEN-D Security Target

Version: v0.9

Author: Grupo Sallén Tech SLU

Date of publication: 2024-02-06

1.2 TOE REFERENCE

TOE Name: ZEN-D + OpenVPN

TOE Developer: Grupo Sallén Tech SLU

TOE Version: ZEN-D v1.2.14.15 + OpenVPN v2.4.4

1.3 TOE OVERVIEW

1.3.1 INTRODUCTION

ZEN-D is cash deposit handling software, designed to give control over Sallén's cash deposit devices. Together with OpenVPN, ZEN-D provide customers with a secure remote management interface. The purpose of the TOE is to offer the user the possibility of making cash deposits in a secure manner. TOE's software modules are designed to give total control over a customer's cash deposit device, as well as managing the hardware with modular technology, and tailored feature packages which allow to add or remove functionalities based on the customer's needs. It can be managed locally using a touchscreen attached to a Sallén cash deposit device, or remotely using secure communication channels connected to an external server application (CashControl) using *Remote Access* functionality. OpenVPN, an open-source software, provides ZEN-D with the required implementations to deploy a secure VPN between the TOE and its management endpoints.

It provides full control:

- Control of financial transactions (deposits and collections).
- Remote management, monitoring and maintenance.
- Remote commands.
- Remote updates.
- Remote configuration.

- Data sent to server in real time.
- Financial data and maintenance data, split between different users.
- Customized integration procedures to reduce time to market.

In addition, the TOE has connections with external USB port and ethernet port.

1.3.2 TOE TYPE

The TOE is composed of the modular software called ZEN-D and the OS service OpenVPNv2.4.4, which are embedded in the ARM board inside a safe manufactured by Sallén. ZEN-D is composed of a backend-frontend application and a set of drivers in charge of orchestrating the Sallén box peripherals. These drivers are also embedded in the ARM board and are considered part of the ZEN-D application.

The OpenVPN service from the Operating System where ZEN-D software runs is considered a TOE component as it is in charge of providing the secure communication functionality. It communicates with CashControl Server and the remote users accessing by Remote Access functionality, in order to remotely manage the safe box by the ZEN-D software.

1.3.3 TOE USAGE & MAJOR SECURITY FEATURES

1.3.3.1 TOE USAGE

ZEN-D is deposit cash handling software, embedded in a Linux-based operative system running over an ARM board designed by Sallén. This software is included in each one of Sallen's deposit units. The TOE manages the deposit unit's hardware and configures and monitors its activity, however, there are some operations that can't be done remotely. Hardware-related management can only be done through the external touchscreen embedded in the safe, whereas configuration and monitoring can be done both remotely and via the touchscreen.

The following hardware-related management functionalities can be performed with ZEN-D:

- **Deposit**: This functionality manages the corresponding hardware with the purpose of letting users deposit cash: only banknotes.
- **Cash In**: This functionality opens the lock from the safe with the purpose of inserting a new cash storage into an empty slot.
- **Open Safe**: This functionality opens the lock from the safe with the purpose of testing its correct performance. (Not to perform a collection).
- **Collection**: This functionality opens the lock from the safe with the purpose of removing a cash storage and registering a new one in the empty slot.
- **Detection System Test**: This functionality allows to perform deposit tests with real banknotes without neither including them in the accountancy nor storing them in the cash storage system.

ZEN-D allows to configure: options menu, system menu, currencies, printer options, network options, user management, device management, cloud management, account management, access control and display off.

As part of its options menu configuration, ZEN-D offers seven login modes for users:

- **Default** mode requests a username, and a password if it's defined, to get into the application.
- **Tiles** shows all the usernames registered in the system. Thereby, the user only has to press on his code to get access to the application.
- **Autologin** activates a default user which logs in automatically after few seconds of inactivity in the main screen.
- **Account + User** once the user inputs an account, it will get all the users associated to that account in order to select its own user.
- **User + Account** is similar to the previous mode, but in this case, the user will be requested before the account number.
- **Multi Deposit** permits to perform several deposits with the same user profile, without need of the user to log in again.
- **User + Card** This login mode requires the user to first introduce their userId and then scan an Id card.

As part of its system menu, settings configuration, ZEN-D offers some additional security-related configuration options:

- **Lock Type** enables extra-security options for CIT company profile:
    - **None** Non-extra security code needed.
    - **Smart Password** A security code generator provided is needed for the smart password generation.
    - **OTC Sallen** One Time Code configuration needed for Sallen OTC lock.
    - **OTC** One Time Code configuration needed for vendor OTC lock.
- **Keep Alive** sets the frequency of heartbeats sent from machine to the cloud servers enabled.
- **Auto Cash Code** it defines how the cash storage codification is registered in the Deposit Platform:
    - **Manual** user shall introduce the cash storage code, either manually or scanning the barcode.
    - **Timestamp** Deposit Platform will assign a code to the cash storage. Code will contain time and date with the format yyyymmddhhmmss.

    - **Device Id Incremental** Deposit Platform will use a correlative number to register the cash storage.
    - **Device Id + Timestamp** It does use the device Id and the timestamp when the cash storage was first inserted to identify the cash storage.
- **Transaction ID Format** defines how the ID transaction is codified:
    - Default.
    - Machine Transaction Number.
    - Device ID + Incremental ID.
    - Location ID + User + Timestamp.
    - Incremental ID + Device ID padded to left.
    - Incremental ID padded to left.
    - Location ID + Time.
    - Cash Storage Transaction Number.

ZEN-D offers the possibility to configure network options:

- **Local Network Type,** where either DHCP or Static IP has to be selected for machine connection.
- **OpenVPN**, which can be enabled/disabled and configured. It is used to provide a communication channel for the remote web-interface management.
- **Cloud management**, allows to configure the settings for the server that is going to be used at customer network for administration, control and monitoring deposit units. The TOE allows the following protocols:
    - Dove: new provider CashControl web socket-based protocol (by default).
    - Cash Deposit System: Legacy Sallén protocol.
    - SafeNet: SafeNet is a software solution for safe deposit systems used at Sallén NL installations.
    - WebDAV: an extension of the Hypertext Transfer Protocol (HTTP) that allows clients to perform remote Web content authoring operations. It's a standard protocol that can be used for managing remotes upgrades from server to deposit machines.
    - FTP: File Transfer Protocol.
    - SFTP: SSH File Transfer Protocol.

In addition, the TOE allows to consult and monitor: deposits, counters, cash content, log viewer, machine status, events pending to be transferred to the cloud server, workflow, daily report and versioning.

1.3.3.2 MAJOR SECURITY FEATURES

The TOE supports the following major security features:

- **Security Audit**. The TOE generates logs for the main events of the application, such as cash movements or user logins, accompanied by a timestamp. These logs can also be reviewed.
- **User Data Protection**. The TOE exercises an access control policy on different users of the application so that not all information can be accessed by all users, and users with less privileges cannot access certain information or sensitive functionalities.
- **Identification and Authentication**. All users that access the TOE are correctly identified and those with security-related privileges that could compromise the assets are authenticated before accessing the TOE.
- **Security Management**. The TOE implements and provides the capability to configure policies that increase product security such as blocking sessions after a time of inactivity, keep alive period, managing cash-related peripherals, querying machine status or blocking the TOE for certain periods of time.
- **TOE Access.** The TOE allows the configuration of an inactivity time for which the user must be authenticated again after this time has elapsed. In addition, the TOE allows the voluntary disconnection of the user who has logged into the TOE, as well as the new login.
- **Trusted Path/Channels**. Communication channels are based in OpenVPN. This protocol guarantees confidentiality, integrity and authentication. It is implemented for both the communication between the TOE and the CashControl application and for the communication between the TOE and the Remote Access functionality accessed by a remote user.

1.3.4 NON-TOE HARDWARE/SOFTWARE/FIRMWARE

Non-TOE components are underlined:

- The TOE is deployed over a Linux-based operating system, Ubuntu 18.04 LTS.
- The OS is embedded in the ARM board LMB_iMX, designed by Sallén.
- The ARM board is inside a safe manufactured by Sallén. The peripherals of this safe model are: printer, bar code reader and an SR120 (an acceptor designed by Sallén, controls the storage unit and the lock) where the driver in charge of handling the SR120 peripheral is part of the TOE. There is a firewall inside the safe which allows communication between the safe and the CashControl application. The TOE can be operated through a physical

touchscreen part of the safe. The TOE operates a lock that protects the cash storage bags. The TOE connects external USB port and ethernet port, which are part of the ARM board.

- It can be operated through a remote computer using the CashControl application.
- An external NTP server provides the TOE with reliable timestamps.
- The TOE application code runs over Node.js service on the Ubuntu 18.04 LTS operating system. Node.js is the engine that provides support to the TOE application code that can be executed by the users through a touchscreen, CashControl application or Remote access functionality.
- SSH channel to access the OS of the machine.

1.4 TOE DESCRIPTION

1.4.1 INTRODUCTION

1.4.1.1 INTRODUCTION

ZEN-D is cash deposit handling software introduced in Sallén's deposit unit. The TOE manages the hardware from the safe and configures and monitors its activity. The ZEN-D application backend is a node.js-based web server that is accepting API REST from a JavaScript-based front-end application.

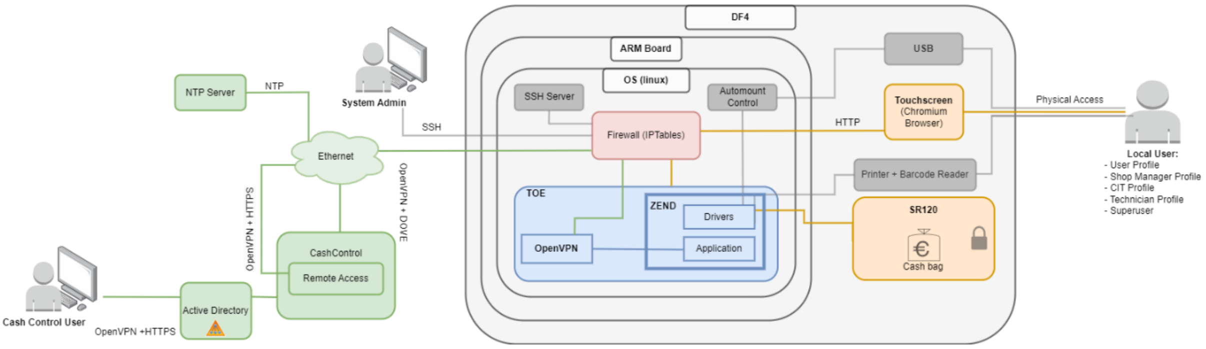

Figure 1 *TOE Scope*

The purpose of the TOE is to offer the user the possibility of making cash deposits in a secure manner. When an administrator with security-related privileges wants to interact with the TOE, an authentication password-based process is done. Actions like successful login are audited and saved to disk. The security of the remote communication channels is based on OpenVPN.

Note: Administrator refers to those TOE users with sufficient privileges to attempt TOE's assets or modify security functionality.

1.4.1.2 TOE EVALUATED CONFIGURATION

The evaluated configuration is defined by the following key points:

- NTP is used to synchronize date and time through an external server. It is configured by default by the manufacturer.
- Login mode is set to default, which requires a user ID as mandatory. Through the security guidelines, a password is required for administrators.
- User roles have assigned the privileges that the application awards them by default.
- Disable firewall functionality is disabled (firewall is activated).
- Lock type is set to Smart Password, which requires an extra security code for performing CIT Collection.
- *Deposit inactivity time* is set by default to 120 (seconds).
- Machine *inactivity time* is set by default to 30 (seconds).
- Keep Alive period is set to 30 (seconds).
- Auto Cash Code is set to Manual.
- Transaction ID Format is set to Location ID + User + Timestamp.
- OpenVPN is correctly configured to connect with the remote management server.
- DOVE protocol is selected as the Cloud management protocol.
- *Downgrade application*, *Set new MAC* and *Reset Serial NO* functionalities are not allowed.
- Workflow modification is not allowed.

1.4.2 TOE LOGICAL SCOPE

The TOE includes several security features. Each of the security features identified above consists of several security functionalities and are considered TOE Security Functionalities, as identified below.

1.4.2.1 SECURITY AUDIT

The TOE generates logs for the main events of the application. The events are recorded with a timestamp, type of event and user that caused the event (if applies). The recorded operations and events are saved as log messages. The TOE provides direct access to logs and the capability of filtering them. Only the role of superuser is able to delete the generated logs.

1.4.2.2 USER DATA PROTECTION

The TOE exercises different policies by default on different roles of the application. The TOE provides six different role types with different privileges and target functionality:

- **User Profile**: This user corresponds with retail store employees. This profile is only allowed to perform cash deposits. This profile can be assigned to different users through user management functionality.

- **Shop Manager Profile**: This user corresponds with a retail store manager. This profile is enabled for configuring and updating the cash deposit machine, managing user profiles (only User Profile and other Shop Manager users) and reviewing deposit information such as amounts, and the type of notes deposited. This profile can be assigned to different users through user management functionality.

- **Technical Profile**: This profile has been created for technicians who install the cash deposit unit, perform maintenance tasks and support the retail stores. Technicians will set up the deposit unit during installation. This profile can be assigned to different users through user management functionality.

- **CIT Profile**: This profile has been created for CIT employees who collect the cash storage and register new cash storage. This profile can be assigned to different users through user management functionality.

- **Superuser**: This profile has been created for the technicians who install the cash deposit unit and has full permissions on all actions and settings that can be carried out on the safe. Therefore, to access as a Superuser, the user must request a smart password from provider personnel. This password is valid for 24 hours. In addition, this role is allowed to define the permissions of all kind of profiles in several menus of the Deposit Platform.

- **CashControl User**: This profile is created by provider personnel to access the CashControl application. It is a user remotely connected to the CashControl server.

  Through the CashControl server, the user sends commands and receives audit information to and from the TOE. The authentication of this user is done against the CashControl server. The connection between the TOE and the server is configured locally on the machine where the TOE is installed.

  In addition, this user can create users of the safe, with the roles described above: User Profile, Shop Manager Profile, CIT Profile and Technician Profile.

Shop Manager Profile, Technical Profile, CIT Profile and Superuser are user roles that are required to enter a password to access. This group of users is therefore defined as TOE Administrators.

1.4.2.3 IDENTIFICATION AND AUTHENTICATION

Identification is done via a User ID. The security guidelines ensure that users with security privileges must create a password for later authentication. Then, the authentication for all profiles (only those with security capabilities that could compromise the assets of the TOE) is done by entering the User ID and its password. Superuser profile's password is generated by vendor personnel and is only valid for 24 hours.

1.4.2.4 SECURITY MANAGEMENT

The TOE implements and provides the capability to configure several functionalities that improve its own security:

- Set deposit inactivity time and application inactivity time. Deposit inactivity Time is the maximum waiting time between a note deposited and the following note deposited in the same deposit. If that time is exceeded, the deposit will conclude automatically. Application Inactivity Time is the longest time without user interaction. In case the limit is reached, the application will come back the main screen and a new login will be requested.

- Machine Status. It shows the current status of unit devices when an error occurs.

- Keep Alive. Sets the frequency of heartbeats sent from machine to the cloud server.

- Ret. Queue. Shows the list of events pending to be transferred to the cloud server. Only data cloud servers can be listed.

- Display off. It allows to set the inactivity schedule for the system, in which it will turn out of service automatically to avoid user interaction.

- Peripheral management through the functionalities related to cash exposure (Cash In, Open Safe and Collection).

- Delete Data operation, that erases all the data excluding the default user profiles and the configuration (except Inactivity time and keep alive periods that are returned to the default value).

- User management: create, modify and delete users attributes.

1.4.2.5 TOE ACCESS

The TOE provides the capability to configure an inactivity time whereby the user must log in or authenticate again, depending on the user role.

In addition, the user has the option to voluntarily log out to close the active session in the TOE. To start a new session the user has to authenticate again. Authentication only applies to users with a user role who must be authenticated.

1.4.2.6 TRUSTED PATH/CHANNELS

There are two communication channels, using the following protocols:

- **Communication between the TOE and the CashControl application**. The OpenVPN protocol is used, which guarantees the confidentiality, integrity and authentication of the communication. In addition, use is made of the DOVE protocol for requests that are executed to the TOE.
- **Communication between the TOE and Remote Access functionality**. The OpenVPN protocol is used, which guarantees the confidentiality, integrity and authentication of

the communication. In addition, use is made of the HTTPS protocol for requests that are executed to the TOE.

1.4.3 TOE PHYSICAL SCOPE

The Target of Evaluation (TOE) includes the following components:

Delivery Item	Type	Description	Version	Delivery Method	Format
ZEN-D	Software	Software that is embedded in the ARM board, which is located inside the safe.	1.2.14.15	Is distributed as an application on the OS that comes on the ARM board. The board is distributed with the safe box and shipped by Courier delivery.	Embedded
SR120 Driver*	Software	Driver used to operate the safe with peripherals, it is located inside the safe.	0.0.0.1	Is distributed as a binary file on the OS that comes on the ARM board. The board is distributed with the safe box and shipped by Courier delivery.	Embedded
OpenVPN	Software	OS service part of the TOE that implements the secure communication channels by	2.4.4	Is distributed as a binary file on the OS that comes on the ARM board. The board is	Embedded

		OpenVPN protocol.		distributed with the safe box and shipped by Courier delivery.	
Preparative Procedures	Preparative Documentation	Documents for the safe acceptance of the TOE and the installation and configuration process.	0.9	Microsoft SharePoint	PDF
Operational User Guidance	Guidance Documentation	Documents describing the safe use of the TOE.	0.8	Microsoft SharePoint	PDF

Table 1 Components of the TOE

* SR120 Drivers consists of several drivers, each with its own version. Therefore, to check the version of SR120 Drivers, it is necessary to check the version of each of the drivers shown in the table below:

SR120 Driver name	**Version**
SR120_MotorControl	1.1.0.6
SR120_HSDS_PS	1.0.0.6
SR120_SafeSeal	3.0.0.7
SR120_Stacker	1.0.0.9
SR120_Bridge	1.0.6.8

SR120_Backup	1.0.0.4
SR120_HSDS_FPGA	1.0.0.2
SR120_Firmwares	1.1.0.61.0.0.63.0.0.71.0.0.91.0.6.81.0.0.41.0.0.2
SR120_Currency1	1.0.1.1
SR120_Check1	1.0.0.0

Table 2 SR120 Drivers

1.5 NON-EVALUATED SECURITY FEATURES

The TOE and its environment are endowed with certain security capabilities that have not been addressed in this evaluation given the characteristics of the security problem.

The TOE is software embedded in an operating system, which implies that the following characteristics have not been evaluated:

- No physical components of the TOE environment (peripheral) have been evaluated. This includes both the SR120 peripheral and its ability to detect genuine banknotes.
- Operating system drivers as intermediaries in the communication between the TOE and the peripherals.
- TOE security capabilities that do not address the threats contemplated: Privilege and workflow management, backups and updates.

2 CONFORMANCE CLAIMS

This Security Target and the TOE described are in accordance with the requirements of Common Criteria 3.1R5.

This Security Target claims conformance with the following parts of Common Criteria:

- Conformance with **[CC31R5P2]**.
- Conformance with **[CC31R5P3]**.

The methodology to be used for the evaluation is described in the "Common Evaluation Methodology" of the Common Criteria standard of April 2017, version 3.1 revision 5 with an evaluation assurance level of EAL2.

This Security Target does not claim conformance with any protection profile.

3 SECURITY PROBLEM DEFINITION

This section describes the security aspects of the operational environment and its expected use in said environment. It includes the declaration of the TOE operational environment that identifies and describes:

- The alleged known threats that will be countered by the TOE.
- The organizational security policies that the TOE has to adhere to.
- The TOE usage assumptions in the suggested operational environment.

3.1 ASSETS

TOE DATA: Configuration data, passwords, logs, economic data, user data and device information.

CASH OPERATIONS: All operations executed that involve cash exposure.

3.2 THREAT AGENTS

REMOTE ATTACKER: Any unauthenticated or unauthorized individual who has access to any part of the communication between the TOE and the node with which it is communicating
Application Note

The nodes with which the TOE communicates are the PC from which the user accesses Cash Control and Cash Control itself. They are considered to be trusted.

TOE USER: A basic user of the TOE that is intended only to perform deposits.

Application note

A basic user of the TOE is a user with not administrative privileges (such as cash retrieval or user management) whose main role is to perform cash deposits.

3.3 THREATS TO SECURITY

This section identifies the threats to assets that require protection by the TOE. The threats are defined in terms of assets concerned, attackers and the adverse action that materializes the threat.

T.UNAUTHORIZED_ACCESS: A **TOE User** locally accessing **Cash Operations** and/or **TOE Data** for which it is not authorized.

A **Remote Attacker** remotely accessing **TOE Data** for which it is not authorized.

T.UNTRUSTED_CHANNELS: A **Remote Attacker** that can listen or intervene in a non-secure communication channel so that it can gain access to **TOE Data**.

3.4 ORGANIZATIONAL SECURITY POLICIES

The organizational Security policies are defined as follows.

P.AUDIT: The TOE shall provide audit functionality: Generation of audit information, storage of audit log and review of audit records.

P.SECURE_FUNCTIONING: The TOE must implement functionalities that allow administrators to know the status of the storage unit, to securely manage its peripherals and functionalities that allow the TOE to be inactive when users do not interact with it.

P.ADMINS_AC: The TOE must implement an access control policy that does not allow any of the administrators to access functionality or resources for which they are not authorized.

3.5 ASSUMPTIONS

The assumptions when using the TOE are the following:

A.SECURE_ENCLOSING: The safe ensures that as long as the TOE does not authorize the opening of the lock where the cash is stored, it is not opened. Moreover, the safe is located in an isolated room which can only be accessed by authorized users.

In addition, the operating system of the machine can be accessed via SSH. This channel is protected by password. Initially, there is a default password which has to be changed as explained in the security guidelines.

A.TIME: The TOE is provided with reliable timestamps through an external NTP server.

A.TRUSTED_ADMIN: All TOE Administrators are trusted and have been trained in security matters. During TOE installation, the administrator rigorously follows the security guidelines.

A.UPDATE: The TOE and its environment is regularly updated with trusted updates to address potential and actual vulnerabilities.

A.SECURE_SERVER: The CashControl server to which the TOE is connected to perform monitoring and maintenance tasks is a cloud-located secure server. It can only be managed by, previously authenticated and authorized TOE Administrators against an Active Directory which is not part of the TOE through a third-party trusted PC (or equivalent). The server is on an isolated network, where each customer has its own OpenVPN-based VPN connection. This ensures that no communication with other servers or safes is available.

The firewall in the TOE's immediate environment prevents incoming and outgoing connections except to those authorized during the normal operation of the TOE and as part of the security guidelines.

4 SECURITY OBJECTIVES

The security objectives are high level declarations, concise and abstract of the solution to the problem exposed in the former section, which counteracts the threats and fulfills the security policies and the assumptions. These consist of:

- the security objectives for the operational environment.
- the security objectives for the TOE.

4.1 SECURITY OBJECTIVES FOR THE TOE

The security objectives for the TOE must determine (to the desired extent) the responsibility of the TOE in countering the threats and in enforcing the OSPs. Each objective must be traced back to aspects of identified threats to be countered by the TOE and to aspects of OSPs to be met by the TOE.

O.AUTHORIZATION: Users must operate the TOE according to their level of privileges, not being able to perform operations or access data to which they are not authorized.

O.AUTHENTICATION: Only properly authenticated users will be able to access privileged TOE functionalities.

O.SECURE_COMMUNICATION: Communication channels shall be secure in order to preserve integrity, authentication and confidentiality from unauthorized third parties.

O.AUDIT: The TOE shall implement auditing so that TSF actions such as login, money movements or changes in the configuration files are saved in logs form.

O.SECURE_FUNCTIONING: The TOE shall implement functionalities that allow Administrators: know the status of the storage unit, secure peripherals management, and to deactivate the TOE when users do not interact with it.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The security objectives for the Operational Environment determine the responsibility of the environment in countering the threats, enforcing the OSPs and upholding the assumptions. Each objective must be traced back to aspects of identified threats to be countered by the environment, to aspects of OSPs to be enforced by the environment and to assumptions to be uphold by the environment.

OE.SECURE_ENCLOSING: The safe shall ensure that as long as the TOE does not authorize the opening of the lock where the cash is stored, it would not be opened. In addition, the safe shall be stored in an isolated physical location with restricted access to authorized users.

The operating system of the machine can be accessed via SSH. This channel is password protected.

Application Note

The evaluation was carried out on an environment consisting of a basic model of the DF4 safe. Since the TOE is the software embedded in the safe, all safes from the manufacturer that guarantee the measures described in the objective are likely to comply with the environment tested in the evaluation.

OE.TIME: The TOE shall be provided with reliable timestamps through an external NTP server.

OE.TRUSTED_ADMIN: All TOE Administrators shall be trusted and trained in security matters. During TOE installation, the administrator shall rigorously follow the security guidelines.

OE.UPDATES: The TOE and its environment shall be regularly updated with trusted updates to address potential and actual vulnerabilities.

OE.SECURE_SERVER: The CashControl server to which the TOE is connected to perform monitoring and maintenance tasks shall be a cloud-located secure server only managed by TOE Administrators through a third-party trusted PC. The server shall be hosted in an isolated network to ensure that Cash Control customers do not have visibility of other clouds than their own.

The firewall in the TOE's immediate environment shall prevent incoming and outgoing connections except to those authorized during the normal operation of the TOE and as part of the security guidelines.

4.3 SECURITY OBJECTIVES RATIONALE

The following table provides a mapping of security objectives tracing each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and 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. This illustrates that the security objectives counter all threats, the security objectives enforce all OSPs and the security objectives for the operational environment uphold all assumptions.

	O.AUTHORIZATION	O.AUTHENTICATION	O.SECURE_COMMUNICATION	O.AUDIT	O.SECURE_FUNCTIONING	OE.SECURE_ENCLOSING	OE.TIME	OE.TRUSTED_ADMIN	OE.UPDATES	OE.SECURE_SERVER
T.UNAUTHORIZED_ACCESS	X	X				X		X		X
T.UNTRUSTED_CHANNELS			X					X		X
P.AUDIT				X			X			
P.SECURE_FUNCTIONING					X					
P.ADMINS_AC	X									
A.SECURE_ENCLOSING						X				
A.TIME							X			
A.TRUSTED_ADMIN								X		
A.UPDATE									X	X
A.SECURE_SERVER										X

Table 3 Security Objectives vs Security Problem Definition

4.3.1 THREATS

T.UNAUTHORIZED_ACCESS: **O.AUTHORIZATION** ensures that the TOE has different levels of privileges for TOE users and administrators.

O.AUTHENTICATION ensures that the user trying to access the TOE with certain privileges is who it claims to be

OE.TRUSTED_ADMIN ensures that the privileges configuration won't be performed in a manner that an administrator provides higher access privileges than expected to unauthorized users. Moreover, administrators with security-related privileges establish a password for accessing the TOE.

OE.SECURE_ENCLOSING This objective ensures that unauthorized access to the operating system of the machine via SSH does not succeed, which could result in obtaining the credentials of the administrators.

OE.SECURE_SERVER ensures that the Ethernet port is protected through the firewall of the TOE's immediate environment against endpoints distinct from CashControl.

T.UNTRUSTED_CHANNELS: **O.SECURE_COMMUNICATION** ensures that the communication channels provide integrity, confidentiality and authentication of the endpoint.

OE.TRUSTED_ADMIN ensures that the configuration of the network communication shall be done according to the guidelines.

OE.SECURE_SERVER ensures that the endpoint of the communication is the trusted CashControl server.

The following table maps the threats of the security problem established to the security objectives of the TOE and the security objectives of the operational environment.

Threats	Security Objectives
T.UNAUTHORIZED_ACCESS	O.AUTHORIZATION O.AUTHENTICATION OE.TRUSTED_ADMIN OE.SECURE_ENCLOSING OE.SECURE_SERVER
T.UNTRUSTED_CHANNELS	O.SECURE_COMMUNICATION OE.TRUSTED_ADMIN OE.SECURE_SERVER

Table 4 Threats vs Security Objectives

4.3.2 ORGANIZATIONAL SECURITY POLICIES

P.AUDIT: **O.AUDIT** ensures that the TOE shall provide the ability to generate, store and review logs.

OE.TIME ensures that the logs are accompanied by a reliable timestamp.

P.SECURE_FUNCTIONING: **O.SECURE_FUNCTIONING** ensures that the TOE provides administrators the functionalities: know the status of the storage unit, secure peripherals management and deactivate the TOE when users do not interact with it.

P.ADMINS_AC: **O.AUTHORIZATION** ensures that no administrator can access resources/assets for which it is not authorized.

The following table maps the organizational security policies of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

OSPs	Security Objectives
P.AUDIT	O.AUDIT OE.TIME
P.SECURE_FUNCTIONING	O.SECURE_FUNCTIONING
P.ADMINS_AC	O.AUTHORIZATION

Table 5 OSPs vs Security Objectives

4.3.3 ASSUMPTIONS

A.SECURE_ENCLOSING: **OE.SECURE_ENCLOSING** ensures there is no cash exposure unless explicitly authorized by the TOE and that the safe is only accessible to authorized users. The SSH channel is protected by password.

A.TIME: **OE.TIME** ensures that an external NTP server provides reliable timestamps to the TOE.

A.TRUSTED_ADMIN: **OE.TRUSTED_ADMIN** ensures that the administrators of the TOE are trusted administrators and that rigorously follow the security guidelines

A.UPDATE: **OE.UPDATES** ensures that the TOE and its environment will be updated if a vulnerability that threat the assets is detected. **OE.SECURE_SERVER** ensures that only authorized updates are installed from the CashControl.

A.SECURE_SERVER: **OE.SECURE_SERVER** ensures that the CashControl server is secure and is only managed by trusted administrators. This objective also guarantees that the server's network is isolated from other CashControl servers.

The following table maps the assumptions of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

Assumptions	Security Objectives
A.SECURE_ENCLOSING	OE.SECURE_ENCLOSING
A.TIME	OE.TIME
A.TRUSTED_ADMIN	OE.TRUSTED_ADMIN
A.UPDATE	OE.UPDATES OE.SECURE_SERVER
A.SECURE_SERVER	OE.SECURE_SERVER

Table 6 Assumptions vs Security Objectives for the Operational Environment

5 EXTENDED COMPONENTS DEFINITION

No extended components have been defined.

6 SECURITY REQUIREMENTS

This section defines the Security functional requirements (SFRs) and the Security assurance requirements (SARs) that fulfill the TOE. Assignment, selection, iteration and refinement operations have been made, adhering to the following conventions:

- Assignments. They appear between square brackets. The word “assignment” is maintained and the resolution is presented in ***boldface, italic and blue color.***

- Selections. They appear between square brackets. The word “selection” is maintained and the resolution is presented in ***boldface, italic and blue color.***

- Iterations. It includes “/” and an “identifier” following requirement identifier that allows to distinguish the iterations of the requirement. Example: FCS_COP.1/XXX.

- Refinements: the text where the refinement has been done is shown ***bold, italic, and light red color.*** Where part of the content of a SFR component has been removed, the removed text is shown in ~~***bold, italic, light red color and crossed out.***~~

6.1 SECURITY FUNCTIONAL REQUIREMENTS

6.1.1 FAU: SECURITY AUDIT

6.1.1.1 FAU_GEN.1: AUDIT DATA GENERATION

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

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

b) All auditable events for the ***[selection: not specified]*** level of audit; and

c) ***[assignment:***
- Accepted or rejected notes
- Login/Logout
- Changes on the status of the unit devices
- Perform cash-related operations
- User management
].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~***PP/***~~ST, ***[assignment: none]***.

6.1.1.2 FAU_GEN.2: USER IDENTITY ASSOCIATION

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Application Note

For Collection, Cash in and Open Safe operations, the superuser ID is not recorded when generating the audit event. Since there is only one superuser and for any other user exercising these operations, their ID is registered, all records of such events that do not contain a user ID are considered to be associated with the superuser.

6.1.1.3 FAU_SAR.1: AUDIT REVIEW

FAU_SAR.1.1 The TSF shall provide ***[assignment: Technical Profile, Shop Manager Profile, Superuser and CashControl user]*** with the capability to read ***[assignment: all the audit data]*** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.3: SELECTABLE AUDIT REVIEW

FAU_SAR.3.1 The TSF shall provide the ability to apply ***[assignment: filtering methods]*** of audit data based on ***[assignment: level and type]***.

6.1.1.5 FAU_STG.1: PROTECTED AUDIT TRAIL STORAGE

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to ***[selection: prevent]*** unauthorized modifications to the stored audit records in the audit trail.

Application Note

Only superuser has the ability to delete audit data. The only way to delete logs is through the *Delete data* functionality.

6.1.2 FDP: USER DATA PROTECTION

6.1.2.1 FDP_ACC.1: SUBSET ACCESS CONTROL

FDP_ACC.1.1 The TSF shall enforce the ***[assignment: Administrator management access SFP]*** on ***[assignment: Subjects – Individual users, Objects – TOE's menus, configurations and functionalities, Operations – Edit, Consult, Operate and Delete]***.

6.1.2.2 FDP_ACF.1: SECURITY ATTRIBUTE BASED ACCESS CONTROL

FDP_ACF.1.1 The TSF shall enforce the ***[assignment: Administrator management access SFP]*** to objects based on the following: ***[assignment: Subjects - Individual users, Objects – TOE's menus, configurations and functionalities, Attributes - User roles]***.

Application Note

The TOE allows security attributes (user roles) to be administered to subjects (users). Administrator management access SFP grants user access to certain objects based on their security attribute. It is set by default as described in the SFR.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[assignment: rules defined by the objects defined in Table 7 which are carried out by the user roles]***.

Application Note

The following table contains a list of security-related management functions controlled under Administrator management access SFP. Since the user profile does not have the capacity to access any of them, it is not included in the table:

Objects\ Security Attribute		Shop Manager Profile	Technical Profile	CIT Profile	Superuser	CashControl User
Audit records		C	C		D/C	C
Security fields configuration[1]			E		E	E
Cash operations (Only locally through touchscreen)	Cash In		O	O	O	
	Collection			O	O	
User Management		E	E/D[2]		E/D	E
Account Management		E	E/D		E/D	
Display off configuration		E/D	E/D		E/D	

Device Management			O		O	
Open Safe (Only locally through touchscreen)			O		O	
Versioning			C		C	
Machine Status		C	C		C	
Special commands	Create Backup Environment				O	
	Ret.Queue		C/D		C/D	
	Access Control				E	
	Workflow		E[3]		E	
	Restart				O	
	Disable Firewall				O	
	Downgrade Application				O	
	Reset Serial NO				O	
	Set new MAC				E	

	Detection System Test		O		O	
	NTP Server Configuration		E		E	O
	Login mode		E		E	E
	Lock-type		E		E	E
	Auto-cash code configuration		E		E	E
	Delete data				O	
	Factory information				O	

Table 7 Subjects and objects controlled under Administrator management access SFP

Operations:

- E: Edit. Where editing involves consulting.
- C: Consult.
- O: Operate. Involves TOE's functionalities and peripherals management.
- D: Delete. The *Delete data* deletion functionality is only accessible by the superuser. Through it, all data stored by the TOE can be deleted. Only profiles defined by default will remain in the device. Configuration won't be deleted (unless Inactivity time and keep alive, which are replaced by their default values). *User management* and *Account Management* objects allow the above-mentioned roles to delete users or accounts independently from the *Delete Data*.

[1] Where security fields configuration refers to the following configurations: Inactivity time configuration, Auto-cleaning configuration, Keep-alive configuration and Network configuration (which includes the configuration of OpenVPN and cloud services). The network configuration cannot be edited by the CashControl user.

[2] The Technical Profile can delete other users, but only with the following roles:

- User Profile
- Shop Manager Profile

[3] The TOE allows the edition of two different workflows flows: Authentication and Deposit. Technical Profile can only Edit Authentication Workflow.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: ***[assignment: None]***.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***[assignment: None]***.

6.1.3 FIA: IDENTIFICATION AND AUTHENTICATION

6.1.3.1 FIA_ATD.1: USER ATTRIBUTE DEFINITION

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: ***[assignment: User role]***.

6.1.3.2 FIA_UAU.2: USER AUTHENTICATION BEFORE ANY ACTION

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

6.1.3.3 FIA_UID.2: USER IDENTIFICATION BEFORE ANY ACTION

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

6.1.4 FMT: SECURITY MANAGEMENT

6.1.4.1 FMT_MOF.1/MODIFICATION: MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

FMT_MOF.1.1/MODIFICATION The TSF shall restrict the ability to ***[selection: modify the behaviour of]*** the functions ***[assignment: objects listed in Table 7 unless those listed in the Application Note below, whose modification is not allowed]*** to ***[assignment: users with specific user role as identified in FDP_ACF.1.1]***.

Application Note

As the Security Guidelines establish, the following functionalities/parameters shall not be executed/modified in order to maintain the certification guarantees:

- NTP server configuration.
- Login mode.
- Access control.
- Disable firewall.
- Lock type.

- Auto Cash Code.
- Transaction ID Format.
- Downgrade application.
- Set New MAC.
- Reset Serial NO.
- Workflows.

6.1.4.2 FMT_MOF.1/DETERMINATION: MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

FMT_MOF.1.1/DETERMINATION The TSF shall restrict the ability to ***[selection: determine the behaviour of]*** the functions ***[assignment: objects listed in Table 7]*** to ***[assignment: user with specific user role as identified in FDP_ACF.1.1]***.

6.1.4.3 FMT_MSA.1: MANAGEMENT OF SECURITY ATTRIBUTES

FMT_MSA.1.1 The TSF shall enforce the ***[assignment: Administrator management access SFP]*** to restrict the ability to ***[selection: modify]*** the security attributes ***[assignment: user roles]*** to ***[assignment: Superuser, Technical Profile, Shop Manager Profile and CashControl User]***.

6.1.4.4 FMT_MSA.3: STATIC ATTRIBUTE INITIALISATION

FMT_MSA.3.1 The TSF shall enforce the ***[assignment: Administrator management access SFP]*** to provide ***[selection: restrictive]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***[assignment: no role]*** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.5 FMT_MTD.1: MANAGEMENT OF TSF DATA

FMT_MTD.1.1 The TSF shall restrict the ability to ***[selection: delete]*** the ***[assignment: all TSF data except configuration and default user roles]*** to ***[assignment: Superuser]***.

6.1.4.6 FMT_SMF.1: SPECIFICATION OF MANAGEMENT FUNCTIONS

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: ***[assignment: - Set deposit inactivity time and application inactivity time***
- Read machine status
- Set the keep alive messages period
- Consult and delete the list of events pending to be transferred to the cloud server (Ret. Queue)
- Set display off periods
- Manage peripherals (cash related)
- Delete data operation
- User Management].

Application note

Although the TOE has functionality to handle drivers for various peripherals, it is not included in the SFR. This is because the operations through drivers that are related to the security of the cash assets are those that involve the opening of the safe door, as these are the scenarios that could involve the exposure of the cash.

6.1.4.7 FMT_SMR.1: SECURITY ROLES

FMT_SMR.1.1 The TSF shall maintain the roles ***[assignment: Shop Manager Profile, User Profile, Technical Profile, CIT Profile, Superuser and CashControl User]***.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5 FTA: TOE ACCESS

6.1.5.1 FTA_SSL.3: TSF-INITIATED TERMINATION

FTA_SSL.3.1 The TSF shall terminate an interactive session after a ***[assignment: time set by the roles with access to this functionality]***.

Application Note

This functionality is only applicable locally, where the user's session is terminated at the end of the configured inactivity time. Not applicable for Remote Access.

6.1.5.2 FTA_SSL.4: USER-INITIATED TERMINATION

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.1.6 FTP: TRUSTED PATH/CHANNELS

6.1.6.1 FTP_ITC.1: INTER-TSF TRUSTED CHANNEL

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[selection: the TSF, another trusted IT product]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***[assignment: -***
Send heartbeats specifying the current status of the machine
- Send financial data: deposits and collections
- Changes in users
- Sending the CashControl server audit data].

6.1.6.2 FTP_TRP.1: TRUSTED PATH

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***[selection: remote]*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from ***[selection: modification, disclosure]***.

FTP_TRP.1.2 The TSF shall permit ***[selection: remote users]*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***[selection: initial user authentication, [assignment: all remote administrative actions]]***.

6.2 SECURITY ASSURANCE REQUIREMENTS

The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements: **EAL2**.

The following table shows the assurance requirements by reference the individual components in **[CC31R5P3]**:

Assurance Class	Assurance Components
ASE: Security Target evaluation	ASE_CCL.1: Conformance claims ASE_ECD.1: Extended components definition ASE_INT.1: ST introduction ASE_TSS.1: TOE summary specification ASE_OBJ.2: Security objectives ASE_REQ.2: Derived security requirements ASE_SPD.1: Security problem definition
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system ALC_CMS.2: Parts of the TOE CM coverage ALC_DEL.1: Delivery procedures
ADV: Development	ADV_ARC.1: Security architecture description ADV_FSP.2: Security-enforcing functional specification ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures
ATE: Tests	ATE_COV.1: Evidence of coverage ATE_FUN.1: Functional testing

Assurance Class	Assurance Components
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 8 Security Assurance Requirements

6.3 SECURITY REQUIREMENTS RATIONALE

6.3.1 NECESSITY AND SUFFICIENCY ANALYSIS

SFR / TOE Security Objective	O.AUTHORIZATION	O.AUTHENTICATION	O.SECURE_COMMUNICATIO N	O.AUDIT	O.SECURE_FUNCTIONING
FAU_GEN.1				X	
FAU_GEN.2				X	
FAU_SAR.1				X	
FAU_SAR.3				X	
FAU_STG.1				X	
FDP_ACC.1	X				
FDP_ACF.1	X				

SFR / TOE Security Objective	O.AUTHORIZATION	O.AUTHENTICATION	O.SECURE_COMMUNICATION	O.AUDIT	O.SECURE_FUNCTIONING
FMT_MSA.1	X				
FMT_MSA.3	X				
FIA_ATD.1	X				
FIA_UAU.2		X			
FMT_MOF.1/Modification					X
FMT_SMF.1					X
FMT_SMR.1	X				
FMT_MTD.1				X	
FTP_TRP.1			X		
FMT_MOF.1/Determination					X
FIA_UID.2		X			
FTP_ITC.1			X		
FTA_SSL.3		X			

SFR / TOE Security Objective	O.AUTHORIZATION	O.AUTHENTICATION	O.SECURE_COMMUNICATION	O.AUDIT	O.SECURE_FUNCTIONING
FTA_SSL.4		X			

Table 9 SFRs / TOE Security Objectives coverage

6.3.2 SECURITY REQUIREMENT SUFFICIENCY

O.AUTHORIZATION: **FDP_ACC.1** defines the ZEN-D's access policy components (Subject, Objects and Operations).

FDP_ACF.1 links every role (subject) with the operations it can perform over an object.

FMT_MSA.1 ensures that Superuser, Technical Profile, Shop Manager Profile and CashControl User roles are able to modify security attributes over roles.

FMT_SMR.1 identifies the different security roles.

FIA_ATD.1 identifies the security attribute belonging to individual users.

FMT_MSA.3 ensures that the TSF provides default authorization levels.

O.AUTHENTICATION: **FIA_UAU.2** ensures that the users are successfully authenticated before using the TOE.

FIA_UID.2 ensures that the users are successfully identified before using the TOE.

FTA_SSL.3 ensures that an interactive session will be locked after a set period of time and only will be unlocked after authentication.

FTA_SSL.4 ensures that the user can voluntarily log out of the session so that a new authentication is required.

O.SECURE_COMMUNICATION: **FTP_TRP.1** ensures that the communication between the TOE and the remote user that execute Remote Access funtionality is secure in terms of confidentiality, integrity and authentication.

FTP_ITC.1 ensures that the communication between the TOE and the CashControl server is secure in terms of confidentiality, integrity and authentication.

O.AUDIT: **FAU_GEN.1** generates audit records for a set of auditable events.

FAU_GEN.2 associates each audit log with a specific user.

FAU_SAR.1 provides the ability for Technical, Shop Manager, Superuser and CashControl User to read the audit records.

FAU_SAR.3 provides the ability to filter the audit records.

FAU_STG.1 ensures that audit storage is protected against modification and/or deletion.

FMT_MTD.1 provides the ability to superuser to delete data, including audit records. The Configuration cannot be deleted.

O.SECURE_FUNCTIONING: **FMT_SMF.1** lists the security management functions that reinforce the security of the TOE in the manner requested in the objective.

FMT_MOF.1/Determination ensures that some roles are able to query the listed management functions.

FMT_MOF.1/Modification ensures that some roles are able to modify the listed management functions.

6.3.3 SFR DEPENDENCY RATIONALE

6.3.3.1 TABLE OF SFR DEPENDENCIES

The following table lists the dependencies for each requirement, indicating how they have been satisfied. The abbreviation "h.a." indicates that the dependency has been satisfied by a SFR that is hierarchically above the required dependency.

SFR	Required	Fulfilled	Missing
FAU_GEN.1	FPT_STM.1	None	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2 (h.a. FIA_UID.1)	None
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	None
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	None
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	None
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	None
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3	None
FMT_MSA.1	FMT_SMR.1, FMT_SMF.1, [FDP_ACC.1 or FDP_IFC.1]	FMT_SMR.1, FMT_SMF.1, FDP_ACC.1	None
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1	None
FIA_ATD.1	None	None	None

SFR	Required	Fulfilled	Missing
FIA_UAU.2	FIA_UID.1	FIA_UID.2 (h.a. FIA_UID.1)	None
FMT_MOF.1/Modification	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None
FMT_SMF.1	None	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2 (h.a. FIA_UID.1)	None
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None
FTP_TRP.1	None	None	None
FMT_MOF.1/Determination	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None
FIA_UID.2	None	None	None
FTP_ITC.1	None	None	None
FTA_SSL.3	None	None	None
FTA_SSL.4	None	None	None

Table 10 SFR Dependencies

6.3.3.2 JUSTIFICATION FOR MISSING DEPENDENCIES

FAU_GEN.1 dependency on FPT_STM.1

The TOE does not provide reliable timestamps. Reliable timestamps are provided by a NTP server which is part of the TOE's environment.

6.3.4 SAR DEPENDENCY RATIONALE

6.3.4.1 TABLE OF SAR DEPENDENCIES

SAR	Required	Fulfilled	Missing
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.2 (hierarchically above ASE_REQ.1)	None
ASE_ECD.1	None	None	None
ASE_INT.1	None	None	None
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	None
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1	None
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.2 (hierarchically above ASE_REQ.1), ADV_FSP.2 (hierarchically above ADV_FSP.1)	None
ALC_CMC.2	ALC_CMS.1	ALC_CMS.2 (hierarchically above ALC_CMS.1)	None
ALC_CMS.2	None	None	None
ADV_FSP.2	ADV_TDS.1	ADV_TDS.1	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.2 (hierarchically above ADV_FSP.1)	None
AGD_PRE.1	None	None	None
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	None
AVA_VAN.2	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	None
ASE_SPD.1	None	None	None

SAR	Required	Fulfilled	Missing
ALC_DEL.1	None	None	None
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	ADV_FSP.2 (hierarchically above ADV_FSP.1), ADV_TDS.1	None
ADV_TDS.1	ADV_FSP.2	ADV_FSP.2	None
ATE_COV.1	ADV_FSP.2, ATE_FUN.1	ADV_FSP.2, ATE_FUN.1	None
ATE_FUN.1	ATE_COV.1	ATE_COV.1	None

Table 11 SAR Dependencies

7 TOE SUMMARY SPECIFICATION

7.1 SECURITY AUDIT (FAU)

7.1.1 FAU_GEN.1 AUDIT DATA GENERATION

The TOE can generate audit records for the events: login and logout, accepted or rejected notes, changes on the status of the machine peripherals (where only SR120 is under the scope of the evaluation), perform cash-related operations (Cash-In, collection and deposits) and user management (creation, deletion or editing). Each audit record has at least a timestamp that identifies the event, type of event and outcome of the event (if the event has been successful, it is recorded). Timestamps are provided by an external NTP server that provides reliable timestamp to the audit record.

7.1.2 FAU_GEN.2 USER IDENTITY ASSOCIATION

Each auditable event that can be attributed to a specific user, is associated with that user. Users are identified with a unique user ID number. Events that can't be associated with a specific user are records that correspond to information related to the cash deposit unit such as cash content and machine status (FAU_GEN.1.1 – "Changes on the status of the unit devices").

For Collection, Cash in and Open Safe operations, the superuser ID is not recorded when generating the audit event.

7.1.3 FAU_SAR.1 AUDIT REVIEW

Superuser, Shop Manager Profile and Technical Profile roles from the TSF are allowed to access audit records. These audit records can be accessed directly through the *Log Viewer* menu. In addition, the TOE periodically sends audits to the CashControl server that can be reviewed by the CashControl User.

7.1.4 FAU_SAR.3 SELECTABLE AUDIT REVIEW

The TOE provides the ability to filter in different manners audit records. *Log viewer* menu allows to perform filter for all audit records. There are two types of filters: by **Type** and by **Level**. The following options are available for each type of filter:

- By **Type**:
    - *All types*.
    - *DepositWorkflow*.
    - *CashStorageWorkflow*.
    - *Authentication*.
    - *UserManagement*.
    - *DeviceManagement*.
    - *Error*.
    - *DepositIncidents*.
    - *Clouds*.

    - *Application*.
- By **Level**:
    - *All levels*.
    - *Info*.
    - *Warning*.
    - *Error*.

7.1.5 **FAU_STG.1** PROTECTED AUDIT TRIAL STORAGE

The only user allowed to perform data deletion is the Superuser and therefore, the TOE protects audit records from unauthorized deletion. On the other hand, the TOE does not provide the capability to perform modifications to the stored audit records.

7.2 USER DATA PROTECTION (FDP)

7.2.1 **FDP_ACC.1** SUBSET ACCESS CONTROL

The following are the operations that can be carried out in the TOE:

- **Consult** refers to having access to and being able to visualize information regarding certain fields such as audit.

- **Edit** refers to the ability to modify TOE settings.

- **Delete** refers to data stored in the TOE, for example audit records or users.

- **Operate** refers on the one hand to the capability of the TOE to execute a direct action on the cash deposit unit that implies the management of peripherals (e.g., opening the lock). In the other hand, models the capability of the user to perform management operations over an object (e.g., restarting the TOE).

Security objects are described below:

- **Audit records**, information concerning to audit records as described **FAU_GEN.1**.

- **NTP Server configuration**, URL and port of the NTP server can be configured. This parameter shall not be modified in order to maintain the certification guarantees.

- **Machine status**, displays the current status of all unit devices, whether an error occurred or the safe is operating correctly.

- **Login mode configuration**, login mode can be selected. This parameter shall not be modified in order to maintain the certification guarantees.

- **Inactivity time configuration**, deposit inactivity Time is the maximum waiting time between a note deposited and the following note deposited in the same deposit. If that time is exceeded, the deposit will conclude automatically. Application Inactivity Time is the longest time without user interaction. In case the limit is reached, the application will come back the main screen and a new login will be requested. These values can be set in seconds.

- **Auto-cleaning configuration**, Auto Cleaning (Months) defines the periodicity in which the information concerning deposits and cash storage registers is deleted. It's set by default in 3 months.

- **Lock-type configuration**, enables extra-security options for CIT company role. This parameter shall not be modified in order to maintain the certification guarantees.

- **Keep-alive configuration**, sets the frequency of heartbeats sent from machine to the cloud servers enabled.

- **Auto-cash code configuration**, it defines how the cash storage codification is registered in the Deposit Platform. This parameter shall not be modified in order to maintain the certification guarantees.

    - **Manual** user shall introduce the cash storage code, either manually or scanning the barcode.

    - **Timestamp** Deposit Platform will assign a code to the cash storage. Code will contain time and date with the format yyyymmddhhmmss.

    - **Device Id Incremental** Deposit Platform will use a correlative number to register the cash storage.

    - **Device Id + Timestamp** It does use the device Id and the timestamp when the cash storage was first inserted to identify the cash storage.

- **Collection**, it is not only used for performing a cash collection but it implies (the workflow itself) that the CIT user should first open the lock, collect the cash storage and register a new cash storage. This workflow can get cut after the cash storage has been extracted but it will imply the TOE stay in a wrong state. (No cash storage registered) and so to get it back to work it would be needed to perform a cash in.

- **Cash in**, used for inserting a new cash storage into an empty slot by opening the lock of the safe.

- **Network configuration**:

    - There are available two types of connections. Depending on customer Network infrastructure, either DHCP or Static IP has to be selected for machine connection.

    - ZEN-D also allows to configure deposit machines on a customer OpenVPN by installing on every machine the certificates and keys for an OpenVPN network. This OpenVPN key can be imported by plugin a USB-stick on the machine USB socket and selecting on the OpenVPN configuration menu.

    - *Cloud Management* menu allows to configure the settings for the server that is going to be used at customer network for administration, control and monitoring deposit units. ZEN-D supports several network protocols:

        - **Dove**: new vendor CashControl web socket-based protocol (by default).

    - **Cash Deposit System**: Legacy Sallén protocol.
    - **SafeNet**: SafeNet is a software solution for safe deposit systems used at Sallén NL installations.
    - **WebDAV**: an extension of the Hypertext Transfer Protocol (HTTP) that allows clients to perform remote Web content authoring operations. It's a standard protocol that can be used for managing remotes upgrades from server to deposit machines.
    - **FTP**: File Transfer Protocol.
    - **SFTP**: SSH File Transfer Protocol.
- **User Management**, allows to create, delete and edit user role profiles at store unit, based on the privileges of the user exercising the action. Main view lists all the profiles created in the system, showing profile features such as: username, User ID, type of role and status.
- **Account Management**, allows to create and manage accounts to gather several usernames. To create an account is needed to define account number, description, holder (owner of the bank account) and currency. Only deposits in currency selected will be permitted in that account.
- **Display off configuration**, allows to set the inactivity schedule for the system, in which it will turn out of service automatically to avoid user interaction.
- **Device management**. This functionality is designed so that in the initial configuration, carried out by a trusted administrator, all the peripherals on which the TOE can operate are detected. This is because the TOE can operate on different safe types with different peripherals.
- **Open Safe**, used for opening the safe without performing cash collection. An extra-security password will be requested before opening the lock, depending on the lock installed.
- **Access control**, it allows to define the permissions of all kind of roles in several menus of the Deposit Platform. This parameter shall not be modified in order to maintain the certification guarantees.
- **Versions**, it displays all the software and firmware versions which devices registered are running with.
- **Workflow**, steps to be followed in deposit, cash in, collection, and authentication operations. They can be added, edited and deleted through its specific menu. There is a default configuration when the cash deposit unit is delivered. This parameter shall not be modified in order to maintain the certification guarantees.
- **Ret.Queue**, shows the list of events pending to be transferred to the cloud server. Only data cloud servers can be listed. Data pending to be transferred can be deleted.

- **Backup environment**, allows to make a backup of the machine configuration that will be stored as backup configuration, so that if the loading of the configuration defined for the machine fails by any chance, this configuration will be used.

- **Delete data**, empties the database by replacing it with a blank database.

- **Restart**, restart the machine.

- **Disable firewall,** disables the firewall allowing any connection to the machine. This parameter shall not be modified in order to maintain the certification guarantees.

- **Downgrade application** performs a downgrade of the application version to the previously installed version. This parameter shall not be modified in order to maintain the certification guarantees.

- **Factory information**, is an option that allows obtaining certain data that will be used later to describe the machine in an ERP (factory level data).

- **Reset Serial NO,** allows to change the serial number of the device. Serial number can be only edited in this menu. This parameter shall not be modified in order to maintain the certification guarantees.

- **Set new MAC,** allows to define and change the MAC address of the deposit unit. MAC address can only be edited in this menu. This parameter shall not be modified in order to maintain the certification guarantees.

- **Detection System Test,** permits to perform deposit tests with real banknotes without neither including them in the accountancy nor storing them in the cash storage system. They are treated as rejected notes**.**

The Security Subjects are the users of the TOE.

7.2.2 FDP_ACF.1 SECURITY ATTRIBUTE BASED ACCESS CONTROL

Each TOE user has assigned a user role, which has a set of privileges associated with it. The security attributes of the subjects are thus the user roles, as specified in **FMT_SMR.1.** A user has different privileges on the defined objects, as collected in *Table 7*.

7.3 IDENTIFICATION AND AUTHENTICATION (FIA)

7.3.1 FIA_ATD.1 USER ATTRIBUTE DEFINITION

Each user registered in the TOE has attached a user role that defines the limits of which menus the specific user can access and what operation is this user allowed to perform in them.

7.3.2 FIA_UAU.2 USER AUTHENTICATION BEFORE ANY ACTION

Given that only roles with administrator privileges (Shop Manager Profile, CIT Profile, Technical Profile and Superuser) have privileges to perform actions that attempt against the TOE's assets, only users with these profiles are obligated to introduce a password; therefore, only administrators are authenticated before any action.

The Shop Manager Profile, Technical Profile and CIT Profile roles are associated with three different users by default. These default users have no password assigned to them. As part of the security guidelines, the administrator initializing the device is forced to set a password to other administrators for accessing the application.

On the other hand, to access with the superuser role, a password must be previously generated (smart password) which will be valid only for 24 hours. This password is randomly generated by an external software depending on the date, the machine to be accessed and the user ID. To get the temporary password for the superuser, the user with this role should contact provider support team to get it.

The TOE configuration is divided into two menus: the system menu and the options menu. The system menu is protected by an additional password. This password is accessible through a menu of Cash Control.

7.3.3 **FIA_UID.2** USER IDENTIFICATION BEFORE ANY ACTION

All users, including basic users, must be identified by introducing an ID number before performing any action.

7.4 SECURITY MANAGEMENT (FMT)

7.4.1 **FMT_MOF.1/MODIFICATION** MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

As described at **FDP_ACF.1**, the TSF allows users depending on their role to modify the value of some of the configurations/functions defined at *Table 7 Subjects and objects controlled under Administrator management access SFP*.

The Modify term is associated to *Edit* (E), parameter described in *Table 7*, **FDP_ACF.1**.

7.4.2 **FMT_MOF.1/DETERMINATION** MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

As described at **FDP_ACF.1**, the TSF allows users depending on their role to query the value of some of the configurations/functions defined at *Table 7 Subjects and objects controlled under Administrator management access SFP*.

The term Determine is associated with *Consult* (C), a parameter described in *Table 7*, **FDP_ACF.1**.

7.4.3 **FMT_MSA.1** MANAGEMENT OF SECURITY ATRIBUTES

Superuser, Technical Profile and Shop Manager Profile role can modify users giving them roles with different permissions over the defined objects by modifying users' privileges.

The CashControl user is a user who remotely accesses the TOE through the server located in Azure. The TOE connects remotely to the server through a process in which the server address is uniquely specified. Once connected, requests made from CashControl are not processed by the access control policy, the user who authenticates against the server has access to all the functionalities implemented from the server. The communication endpoints are authenticated through signed certificates, and the messages exchanged are protected in terms of authentication, integrity and confidentiality.

The CashControl User has the functionality to create new users in the TOE. These have a role of the safe assigned to them: User Profile, Technical Profile, Shop Manager Profile and CIT Profile. The following table (*Table 12*) lists the default permissions that each role has in user management. All marked users will be able to create, edit and delete users under the allowed roles (except for the Shop Manager Profile, who cannot delete another Shop Manager Profile nor User Profile).

		Roles to be managed				
		User Profile	**Technical Profile**	**CIT Profile**	**Shop Manager Profile**	**Superuser**
Role	**User Profile**					
	Technical Profile	X			X	
	CIT Profile					
	Shop Manager Profile	X			X	
	Superuser	X	X	X	X	

Table 12 User roles to be created

7.4.4 FMT_MSA.3 STATIC ATTRIBUTE INITIALISATION

ZEN-D has default security attributes as it has default user roles with default permissions to perform different operations. No role is authorized to specify a different value than the default value for each user role. The TOE does not allow to create a user without specifying its role, and the role shall be one between User Profile, Shop Manager Profile, Technical Profile or CIT Profile.

7.4.5 FMT_MTD.1 MANAGEMENT OF TSF DATA

The Superuser role is able to remove all the data of the device such as: profiles created, deposits performed, cash storages registered and log activity. Only profiles defined by default remain in the device. Configuration is not deleted unless Inactivity time and keep alive, which are replaced by their default values.

7.4.6 FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS

This SFR lists the management functions that the TOE implements in order to increase its security.

- Set Deposit Inactivity Time, deposit inactivity time is the maximum waiting time between a note deposited and the following note deposited in the same deposit. If that time is exceeded, the deposit will conclude automatically. Application Inactivity Time is the longest time without user interaction. In case the limit is reached, the application will come back the main screen and a new login will be requested. These values are set in seconds. As the evaluated configuration, their values are set to default. Inactivity times can be modified, the security guidelines ensure that set times do not exceed those established in the evaluated configuration.

- Consult machine status shows the status of all unit devices. In addition, it is sent to CashControl when audit events occur.

- Set keep alive message period, sets the frequency of heartbeats sent from machine to the cloud servers enabled. Keep alive period can be modified, the security guidelines ensure that set period do not exceed the one established in the evaluated configuration.

- Consult and delete the list of events pending to be transferred to the cloud server, this is done though the Ret. Queue menu.

- Set display off periods, allows to set the inactivity schedule for the system, in which it will turn out of service automatically to avoid user interaction.

- Manage peripherals, refers to the TOE's ability to handle and receive information from the peripherals through its drivers. The peripherals that the TOE can handle are: printer and SR120. However, only SR120 is under the scope of the evaluation, since are the only peripherals whose security affect the TOE's assets.

- Perform delete data operation, it erases all the data of the device such as: profiles created, deposits performed, cash storages registered and log activity. Only profiles defined by defect will remain in the device. Configuration is not deleted unless Inactivity time and keep alive, which are replaced by their default values.

- User management refers to the ability of an administrator create, modify and delete user's attributes (username, role, name, language, password, external user ID and status).

7.4.7 **FMT_SMR.1** SECURITY ROLES

- User Profile, corresponds with retail store employees. This profile is only allowed to perform cash deposits.

- Shop Manager Profile, corresponds with a retail store manager. It is capable of managing user profiles (only User Profile and others Shop Managers) , display off periods and reviewing deposit information such as amounts, and kind of notes deposited.

- Technical Profile, technicians who install the cash deposit unit, perform maintenance tasks and support the retail stores. Technicians set up the deposit unit during installation.

- CIT Profile, CIT employees who collect the cash storages and register new cash storages.

- Superuser, technicians who install the cash deposit unit, has full permissions on all actions and settings that can be carried out on the safe. Technicians will set up the deposit unit during installation. The access to this deposit unit is secured by a dynamic password which must be generated with an external software. To obtain the password it is necessary to contact provider support team, which will provide the password valid for 24 hours.
- CashControl User, corresponds with remote users who can access the safe via the CashControl application. The credentials of these users are provided by Sallen's personnel.

7.5 TOE ACCESS (FTA)

7.5.1 **FTA_SSL.3** TSF-INITIATED TERMINATION

The functionality *inactivity time configuration* provides the TOE with the ability to set an inactivity time after which the user must log in/authenticate again, depending on its role.

Remote Access does not allow inactivity time, it is only available locally. Therefore, the user's session is terminated at the end of the inactivity time only accessing the TOE locally through the TouchScreen interface.

Application inactivity time is not applicable to users with the role User Profile since its only functionality is to perform deposits whose inactivity is controlled by *Deposit inactivity time*.

7.5.2 **FTA_SSL.4** USER-INITIATED TERMINATION

The user can voluntarily logout to close the active session in the TOE. In this way, to start a new session the user will have to authenticate again. Authentication only applies to those users with a user role that must be authenticated, otherwise the user only must identify itself (user role).

Administrators have a logout button with which to execute the functionality while users with the User Profile role have to complete a deposit flow or wait for the deposit inactivity time.

7.6 TRUSTED PATH/CHANNELS (FTP)

7.6.1. **FTP_ITC.1** INTER-TSF TRUSTED CHANNEL

The TOE can be operated through a remote computer using CashControl application. The application is deployed in Azure cloud services and is designed to monitor and manage certain specific functionalities of a set of units. It allows to execute functionalities that are applicable to a set of devices, so that they can be managed following similar policies. In addition, the TOE sends audit information to the application. The TOE and CashControl need to be in the same network. This is achieved by using a OpenVPN connection to the Azure server configured prior to acceptance by the developer.

To gain access from the CashControl application, it is necessary to configure the cloud management as described in the evaluated configuration, which implies that the DOVE protocol is selected as the communication protocol with the server. DOVE protocol must first be enabled on the server. Access to the CashControl application requires prior authentication. This authentication is done against an Active Directory handling the management users in CashControl, which is not part of the TOE.

As part of the establishment of the communication channel OpenVPN establishes a control channel based on TLS v1.2 using secure cipher suites in order to handle authentication, key negotiation, and configuration subsequently used by the OpenVPN data channel. In this control channel, the TOE acts as TLS client and the cipher suite that implements is TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. The user authentication against the OpenVPN server is done by user and password.

When the control channel is successfully stablished through TLS 1.2, OpenVPN stablishes a data channel that is protected in authentication, modification and disclosure. Confidentiality is ensured using AES-256-CBC, and both integrity and message authentication are guaranteed using HMAC-SHA-1 (both algorithms implemented by the TOE). OpenVPN uses dynamically compiled OpenSSL v1.1.0g to support its cryptographic functionality.

Note that HMAC-SHA-1 in the current use case is declared as a legacy mechanism by [SOG-IS] and [STIC-807].

**Legacy mechanisms that are deployed on a large scale, currently offer a security level of at least 100 bits and are considered to provide an acceptable short-term security, but should be phased out as soon as practical because they do no longer fully reflect the state of the art and suffer from some security assurance limitations as compared with recommended mechanisms. As a consequence, a validity period is defined for legacy mechanisms. Refer to [SOG-IS] section 1.1 for additional information.*

Once the CashControl application has been accessed, it allows to request Remote access for individual units.

7.6.2. **FTP_TRP.1** TRUSTED PATH

To enable remote access, it is necessary to establish a OpenVPN connection by importing the cryptographic keys to the TOE and configuring the TOE. Once the connection is established through OpenVPN v2.4.4, the remote access functionality can be exercised. The remote interface is similar to the one offered by the touchscreen locally, since it has access to the ZEN-D frontend application. They differ in that there are certain functionalities that cannot be exercised remotely (as shown in the table below).

As part of the establishment of the communication channel OpenVPN establishes a control channel based on TLS v1.2 using secure cipher suites in order to handle authentication, key negotiation, and configuration subsequently used by the OpenVPN data channel. In this control channel, the TOE acts as TLS client and the cipher suite that implements is TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384. The user authentication against the OpenVPN server is done by user and password.

When the control channel is successfully stablished through TLS 1.2, OpenVPN stablishes a data channel that is protected in authentication, modification and disclosure. Confidentiality is ensured using AES-256-CBC, and both integrity and message authentication are guaranteed using HMAC-SHA-1 (both algorithms implemented by the TOE). OpenVPN uses dynamically compiled OpenSSL v1.1.0g to support its cryptographic functionality.

Note that HMAC-SHA-1 in the current use case is declared as a legacy mechanism by [SOG-IS] and [STIC-807].

**Legacy mechanisms that are deployed on a large scale, currently offer a security level of at least 100 bits and are considered to provide an acceptable short-term security, but should be phased out as soon as practical because they do no longer fully reflect the state of the art and suffer from some security assurance limitations as compared with recommended mechanisms. As a consequence, a validity period is defined for legacy mechanisms. Refer to [SOG-IS] section 1.1 for additional information.*

When using remote access, CIT Profile and User Profile are restricted during the execution of the login process where a check is made to see if a remote connection is being made. If the answer is yes, the login process is terminated and the user is blocked with the response *the user does not exist*.

Actions that users can perform are similarly restricted when the check of whether a remote connection is being made is positive. Thus, when the actions available to the user in the main menu are requested, only those that can be performed when the connection is identified as remote are returned. In this case the user actions not shown are the following per user:

User role	Actions blocked for remote connection
Superuser	• Collection • Cash in • Open safe • Detection system test
Technical Profile	• Cash In • Open Safe • Detection system test
Shop Manager Profile	• Start deposit

Table 13 Users actions blocked for remote connection

8 ACRONYMS

The following table shows the acronyms used in this document.

Acronym	Meaning
PP	Protection Profile
CC	Common Criteria
TSFi	TSF Interface
OSP	Organizational Security Policies
EAL	Evaluation Assurance Level
ST	Security Target
IT	Information Technology
ARM	Advanced RISC Machine
SFP	Security Function Policy
DHCP	Dynamic Host Configuration Protocol
IP	Internet Protocol
HTTP	Hypertext Transfer Protocol
SFTP	SSH File Transfer Protocol
NTP	Network Time Protocol
TSF	TOE Security Functionality
TOE	Target of Evaluation
ERP	Enterprise Resource Planning
FTP	File Transfer Protocol
VPN	Virtual Private Network
USB	Universal Serial Bus
OTC	One Time Code
SSH	Secure Shell
OS	Operating System
API	Application Programming Interface
MAC	Media Access Control
PGP	Pretty Good Privacy
URL	Uniform Resource Locators
CIT	Cash In Transit

Table 14 Abbreviations

9 GLOSSARY OF TERMS

Term	Meaning
Augmentation	Addition of one or more requirement(s) to a package
Evaluation Assurance Level	Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
Operational Environment	Environment in which the TOE is operated
Protection Profile	Implementation-independent statement of security needs for a TOE type
Security Target	Implementation-dependent statement of security needs for a specific identified TOE
Target Of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance

Table 15 Glossary of terms

10 DOCUMENT REFERENCES

The following table shows the references used in this document.

Reference	Document
[CC31R5P1]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 1: Introduction and general model
[CC31R5P2]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 2: Security functional components
[CC31R5P3]	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 3: Security assurance components
[CEM31R5P3]	Common Criteria Evaluation methodology, Version 3.1, Revision 5
[SOG-IS]	SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms. Version 1.2. January 2020
[STIC-807]	Guía de Seguridad de las TIC CCN-STIC 807. Criptología de empleo en el Esquema Nacional de Seguridad. May 2022

Table 16 List of document references