



BOOLEBOX ON PREMISES V. 4.2

Security Target

V. 1.5

REVISION HISTORY

Version	Modification Date	Description of changes
1.0	2018-07-09	First Issue
1.1	2018-12-10	Revision to answer ROA_01
1.2	2019-05-17	Revision to answer ROA_02 and ROA03
1.3	2019-08-05	Revision to answer ROA_02 and ROA_04
1.4	2019-10-29	Revision to answer ROA_05
1.5	2020-02-21	Revision to answer ROA_06 and ROA_07

TABLES OF CONTENTS

REVISION HISTORY	2
REFERENCES.....	6
DOCUMENT TERMINOLOGY	7
1 ST INTRODUCTION	8
1.1. ST REFERENCE.....	8
1.2. TOE REFERENCE.....	8
1.3. DOCUMENT ORGANIZATION	8
1.4. DOCUMENT CONVENTIONS	9
1.5. TOE OVERVIEW.....	9
1.5.1. USAGE OF THE TOE	9
1.5.2. MAJOR SECURITY FEATURES OF THE TOE.....	11
1.5.3. TOE TYPE	16
1.5.4. REQUIRED NON-TOE COMPONENTS.....	17
1.5.4.1. SERVER SIDE.....	17
1.5.4.2. END USER SIDE.....	17
1.6. TOE DESCRIPTION.....	18
1.6.1. TOE USERS PROFILES.....	20
1.6.2. PHYSICAL SCOPE OF THE TOE	20
1.6.3. LOGICAL SCOPE OF THE TOE	20
1.6.4. TOE GUIDANCE DOCUMENTATION.....	22
1.6.5. USER DATA AND TSF DATA HANDLED BY THE TOE	22
2 CONFORMANCE CLAIM	22
2.1. CC CONFORMANCE CLAIM	22
2.2. PP CONFORMANCE CLAIM	22
3 SECURITY PROBLEM DEFINITION.....	23
3.1. THREATS	24
3.2. ORGANISATIONAL SECURITY POLICIES.....	25
3.3. ASSUMPTIONS	26
4 SECURITY OBJECTIVE	27
4.1. SECURITY OBJECTIVES FOR THE TOE	27
4.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT.....	28
4.3. SECURITY OBJECTIVES RATIONALE	30
5 EXTENDED COMPONENTS DEFINITION	38
5.1. EXTENDED COMPONENTS DEFINITION	38
6 SECURITY REQUIREMENTS.....	39
6.1. SECURITY FUNCTIONAL REQUIREMENTS	39
6.1.1. SECURITY AUDIT.....	41
6.1.2. IDENTIFICATION AND AUTHENTICATION	43
6.1.3. USER DATA PROTECTION	45
6.1.4. PROTECTION OF THE TSF	55
6.1.5. SECURITY MANAGEMENT	56
6.1.6. PRIVACY	60
6.2. SECURITY ASSURANCE REQUIREMENTS.....	61

6.3. SECURITY FUNCTIONAL REQUIREMENTS RATIONALE 62

 6.3.1. CC Component Dependencies 62

 6.3.2. Tracing between SFRs and the security objectives for the TOE 65

7 TOE SUMMARY SPECIFICATION 68

 7.1. SECURITY FUNCTION 68

 7.1.1. SF_1: Identification and Authentication 68

 7.1.2. SF_2: Security Audit 69

 7.1.3. SF_3: USER data and TSF data protection 71

 7.1.4. SF_4: Security Management 74

 7.1.5. SF_5 Access Control 80

 7.1.6. SF_6 Privacy 83

 7.2. TOE SUMMARY SPECIFICATION RATIONALE 83

LIST OF TABLES

Table 1: Terms and Acronyms used in Security Target 7

Table 2: ST Reference 8

Table 3: ST Organization and Section Descriptions 8

Table 4: Minimum SW and HW prerequisites – server side 17

Table 5: Software prerequisites – end user side 17

Table 6: Threats 24

Table 7: Organizational Security Policies 25

Table 8: Assumptions 27

Table 9: Security Objectives for the TOE 28

Table 10: Security objectives for the operational environment 29

Table 11: Tracing between security objectives for the TOE and security objectives for the Operational Environment vs Threat, OSP and Assumption 31

Table 12: Rationale for Mapping of Threats, Policies, and Assumptions to Objectives 37

Table 13: List of SFR and related operations 40

Table 14: User Privileges 44

Table 15: BBOP Administrators access control SFP 46

Table 16: BBOP Users access control SFP 47

Table 17: uploaded file access control SFP 48

Table 18: file sharing permissions configurable in a sharing template 49

Table 19: BooleBox flow control SFP 52

Table 20: list of properties of the external entities 55

Table 21: Management of TSF data 56

Table 22: Management of security functions 57

Table 23: Management of security attributes 57

Table 24: Management of security attributes 58

Table 25: Management of security attributes 58

Table 26: Security Assurance Requirements 61

Table 27: TOE SFR dependency rationale 64

Table 28: Mapping of TOE SFRs to Security Objectives 65

Table 29: Rationale for TOE Security Objectives coverage by SFRs 67

Table 30: Category of Security Relevant Auditable Events for Administrative profile 69

Table 31: Category of Security relevant Auditable Events for USR profile 70

Table 32: TOE Security Functions/SFRs mapping 83

Table 33: SFR to TSF rationale 85

LIST OF FIGURES

Figure 1: BooleBox On Premises V 4.2 High Level Architecture	10
Figure 2: Typical usage of BooleBox On Premises V 4.2 within customer infrastructure architecture	11
Figure 3: steps for information encryption at rest	12
Figure 4: Product categories covered by BooleBox	16
Figure 5: TOE components and Dashboard parameter settings	19
Figure 6: Boole Box flow control policy scheme	50
Figure 7: MASTER KEY creation process	71
Figure 8: file encryption process	72
Figure 9: file decryption process	73
Figure 10: The Dashboard	74
Figure 11: Classification Project creation	77
Figure 12: Classification Project configuration	77
Figure 13: The Control Panel	78
Figure 14: Example of end-user settings	82

REFERENCES

- [CCP1] CCMB-2017-04-001 - Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, ver. 3.1 Revision 5, April 2017.
- [CCP2] CCMB-2017-04-002 - Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, ver. 3.1 Revision 5, April 2017.
- [CCP3] CCMB-2017-04-003 - Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, ver. 3.1 Revision 5, April 2017.
- [CEM] CCMB-2017-04-004 - Common Methodology for Information Technology Security Evaluation - Evaluation Methodology, ver. 3.1 Revision 5, April 2017.

DOCUMENT TERMINOLOGY

TERM	DEFINITION
ADM	Administrator role
ADR	Administrative Restricted role
AUTHORIZED ADMINISTRATOR	Administrative TOE user with the permission to access a specific section of the dashboard and to use a specific TOE security functionality
CC	Common Criteria (ISO/IEC 15408) Version 3.1 Rev. 5. www.commoncriteriaportal.org/cc
DBMS	DataBase Management System
EAL	Evaluation Assurance Level
GUEST	Guest role
IT	Information Technology
OS	Operating System
OSP	Organizational Security Policy
OTP	One-time password
PERSONAL KEY	Alphanumeric string of variable length used by the TOE in the process AES256 key generation
SAM	Super Administrator role
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
STORAGE	Space where the encrypted data are saved. It can be provided by the Operating System Microsoft Windows Server 2016 by storing data on the server's file system or by a dedicated external HW unit (for example, NAS).
TOE	Target of Evaluation. In the following chapters Target of Evaluation (TOE) stands for BOOLEBOX ON PREMISES V 4.2.
TSF	TOE Security Functions
TSF DATA	Data in a TOE is categorized as either user data or TSF data. TSF Data is information used by the TSF in making decisions as required by the SFRs. TSF Data may be influenced by users if allowed by the SFRs. Security attributes, authentication data, TSF internal status variables used by the rules defined in the SFRs or used for the protection of the TSF and access control list entries are examples of TSF data.
TSFI	TOE Security Functionality Interfaces
UPLOADED DATA	File archived in Boole Box by a TOE user. Synonym of uploaded file in this document.
USR	User role
USER DATA	Data in a TOE is categorized as either user data or TSF data. User Data is information stored in TOE resources that can be operated upon by users in accordance with the SFRs and upon which the TSF places no special meaning. For example, the content of an electronic mail message is user data.

Table 1: Terms and Acronyms used in Security Target

1 ST INTRODUCTION

1.1. ST REFERENCE

[1]

Title:	<i>BooleBox On Premises V 4.2 Security Target</i>
Version:	<i>1.5</i>
Date:	<i>2020-02-06</i>
Assurance Level:	<i>EAL 2 augmented with ALC_FLR.2</i>
CC Version:	<i>Common Criteria v.3.1 Revision 5</i>
Author:	<i>Boole Server S.r.l.</i>

Table 2: ST Reference

1.2. TOE REFERENCE

[2] The TOE is the software product: **BooleBox On Premises V 4.2.**

1.3. DOCUMENT ORGANIZATION

[3] This Security Target follows the following format:

Section	Title	Description
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives counter the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 3: ST Organization and Section Descriptions

1.4. DOCUMENT CONVENTIONS

- [4] The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 rev. 5 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are refinement, selection, assignment and iteration.
- The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by showing the value in italics bold green text (example: *assignment_value(s)*).
 - The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements are indicated using green bolded text for additions (Example: **TSF**), and strike-through for deletions (Example: ~~TSF~~).
 - The **selection** operation is picking one or more items from a list to narrow the scope of a component element. Selections are denoted by underlined bold italicized green text (Example: *selected_value(s)*).
 - **Iteration**: Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_XXX.1.1 (1) and FIA_XXX.1.1 (2) refer to separate instances of the FIA_XXX.1 security functional requirement component.

1.5. TOE OVERVIEW

- [5] BooleBox On Premises 4.2 (i.e. the TOE, or BooleBox or BBOP in the rest of the document) is a **secure file sync and share solution**, purposely designed for individuals and businesses who have sensitive data they need to protect. Unlike typical file sharing services, BooleBox offers complete privacy and control over their data with Personal Keys encryption and data controls, without compromising the usability.
- [6] BBOP ensures that data cannot be lost or stolen when in transit or stored.
- [7] BBOP can protect any type of data file, including presentations, documents, images, spread sheets, etc. and enables the owner to control how others may use the information. With BBOP it is possible to enforce which users are authorized to access the data and control how, when and for how long they may do so. Through BBOP a customer organization can store sensitive data and information within its company, applying the strictest security standards.

1.5.1. USAGE OF THE TOE

- [8] BooleBox empowers organizations to choose how they store and share confidential information. BooleBox protects company's data from external attacks and insider theft, through encryption.
- [9] BBOP is designed to protect against unauthorized viewing, manipulation or distribution of confidential data: it manages data protection, encryption, all information related to user profiles and their rights to access and use shared files.
This comprehensive, controlled approach allows organizations with BooleBox to focus on:
- control of data confidentiality and integrity
 - protection of intellectual property
 - customizable rights with differentiated access to information
 - audit of the operations that users perform on files.

[10] BBOP Users can access all its functionalities via any internet browser.

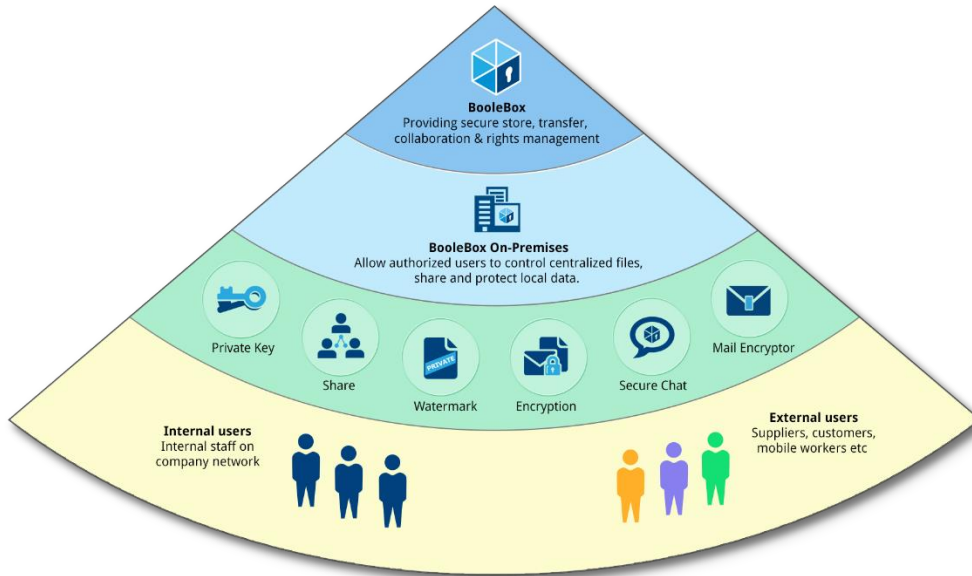


Figure 1: BooleBox On Premises V 4.2 High Level Architecture

- [11] Through its workspace a user can:
- Centrally store and protect files and folders
 - Share information in a temporary way and with granular permission rights
 - Create and control data access profile (classification project)
 - Monitor the activities performed by users on protected information
 - Send and receive encrypted email messages
 - View files in protected mode
 - direct links to access centralized protected information
 - view stored documents directly through the web browser or download them.

[12] **Typical usage of BooleBox within customer infrastructure architecture**

[13] BooleBox can be used in “Standard (not redundant)” as well as in “High Availability (HA)” configurations.

[14] As a general best practice, it is recommended to have separate servers for BooleBox application, BooleBox storage and BooleBox database, as depicted in the following figure.

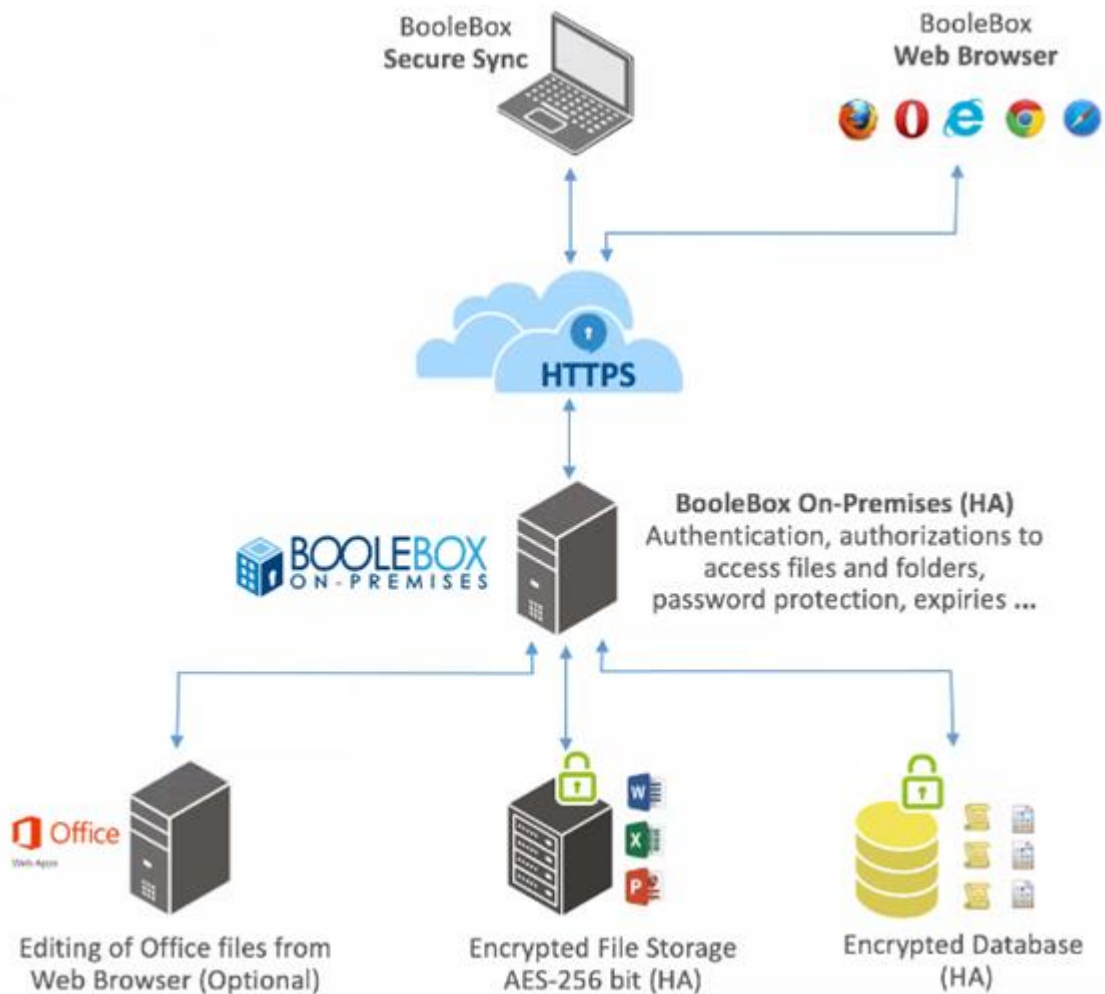


Figure 2: Typical usage of BooleBox On Premises V 4.2 within customer infrastructure architecture

1.5.2. MAJOR SECURITY FEATURES OF THE TOE

[15] The major security features offered by the BooleBox On Premises 4.2 are summarized below.

[16] **TOE users unique Identification & Authentication with Strong authentication and Access from unsecure devices management option**

User access to BooleBox is based on: $\{user_id; user_password\}$ where the *user_password* must satisfy complexity criteria as configured by an authorized administrator, according to the organization password policy, granting as a minimum that:

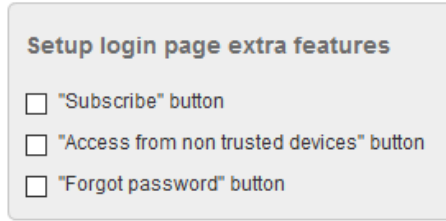
- Password minimum length is 8 characters
- Password must contain at least one uppercase letter
- Password must contain at least one lowercase letter
- Password must contain at least one numeric character.

To further secure the login phase, BooleBox is configured by authorized administrators to force user's identity Two-Step Verification: users will then receive on their mobile a one-time-password valid for one single access.

Here below are listed additional login options that, whether configured by an authorized

administrator, are valid for each user:

Login Options



“subscribe” button:

When checked it means that the users will be asked (una tantum) to register, providing their personal data, before accessing BBOP services.

“access from non-trusted devices” button

When checked it means that the users, that must have provided their email, will be allowed to access BBOP from unsecure devices: in case of login from untrusted device, users will then receive on their mobile a one-time-password valid for one single access. In the certified version of the product the "access from non trusted device" login option is not shown to the TOE user as the OTP is in any case sent to the user except for the Guest user.

“forgot password” button

When checked it means that the users will be provided, in the login mask, with a button to request the forgotten password. By clicking on "forgotten password" the user must enter the e-mail address linked to his account and wait for the password recovery e-mail. The user can then create a new password and log in to his / her private area.

[17] **Uploaded Information encryption at rest**

BBOP grants that your archive is a truly protected space that can be accessed externally and internally in a controlled manner: data at rest are encrypted using 256-bit AES.

BooleBox uses the encryption algorithm 256-bit AES offered by the underlying operating system, in the block cipher symmetric-key method.

- 1 - Upload of file split into 1024-byte blocks
- 2 - Encryption of the blocks using a key derived from user’s PERSONAL KEY or BB MASTER KEY, that is installed on BBOP server and stored encrypted with the K_{pub} on the certificate uploaded during BBOP setup.
- 3 - The storage receives the file blocks and archives the whole encrypted file.

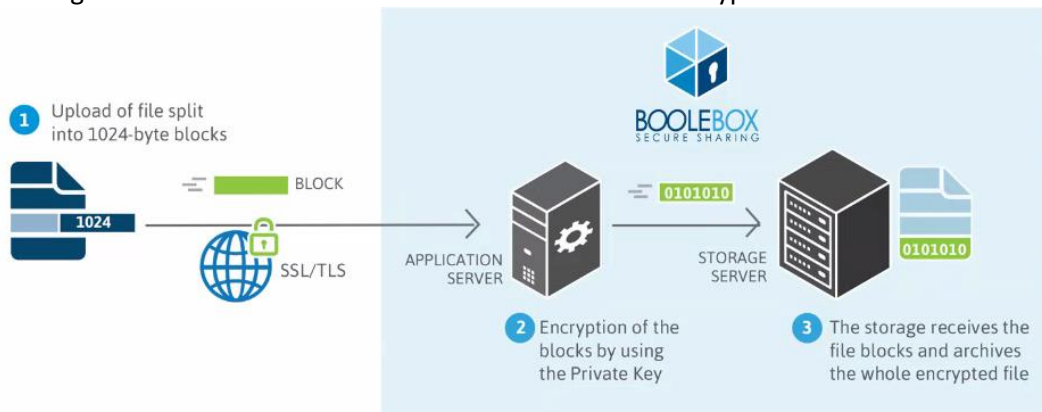


Figure 3: steps for information encryption at rest

BooleBox uses a different randomly generated MASTER KEY for each installation. The random generation functionality (RNG) is provided by the operational environment (Microsoft .Net GUIDE + CNG - Cryptography API: Next Generation) Features.

[18] **Personal Encryption Keys**

By default users data are encrypted with BBOP MASTER KEY, that differs for each BBOP installation and it is stored encrypted.

Alternatively, users can choose and set their own Personal Encryption Keys on their data, to make them even more secure.

When users set a Personal Key to protect their data in BooleBox (i.e. single, multiple files, folders or e-mails), they have only to type it in a relevant field (personal keys defined by users shall satisfy the same complexity criteria as defined for users' passwords): from that moment, BooleBox will use that key instead of the MASTER KEY to encrypt the data. Hence, anytime users want to access a file protected by the Personal Key, they will be asked to type it in; if correct, BooleBox will be able to decrypt the file.

BooleBox doesn't store Personal Encryption Keys in anyway (nor encrypted, neither in clear), but it uses it to generate the AES256 Key to encrypt users' data.

According to classification template settings, BooleBox protects file contents even when viewed in clear for example from screenshot, video grabbing, copy and paste.

[19] **Secure exchange (Information encryption in transit)**

BooleBox offers you, with the support of the underlying operating system, a file-sharing system that is fully protected against external attacks and internal theft: BooleBox uses Transport Layer Security (TLS 1.2), offered by the underlying operating system, for data transfer creating a secure tunnel protected by 256-bit Advanced Encryption Standard (AES) encryption.

Data transferred are encrypted, as a result any intercepted data is impossible to view.

[20] **Protected e-mail**

BooleBox does allows users to send and receive confidential information through e-mail in total security. With BooleBox it is possible to attach confidential documents to e-mails with the assurance that no one can intercept since the email message itself is encrypted or read them, except from authorized e-mail recipients.

With BooleBox e-mail encryption system, you can exchange sensitive information in encrypted mode and revoke access authorization even after sending.

[21] **Anti-Capture & Deter Photo Shots**

BooleBox ensures the data confidentiality not only when it is transferred and stored online. BooleBox persistently protects data, even when it is being used. Advanced security features, such as Anti-Capture and Deter Photo Shots reduce risks related to screen capture activities (through Print Screen system functionalities and video grabbing software) while viewing confidential documents.

The Windows OS is indispensable on the END USER side in order to use this security function.

[22] **Controlled data management (file classification)**

Data and documents are exposed to risks both externally and within a work group. With BooleBox, users can have maximum control of data and its access, as data can be classified and protected even from registered users. With BooleBox, users can apply your protection rules (encryption & access) automatically based on data classification.

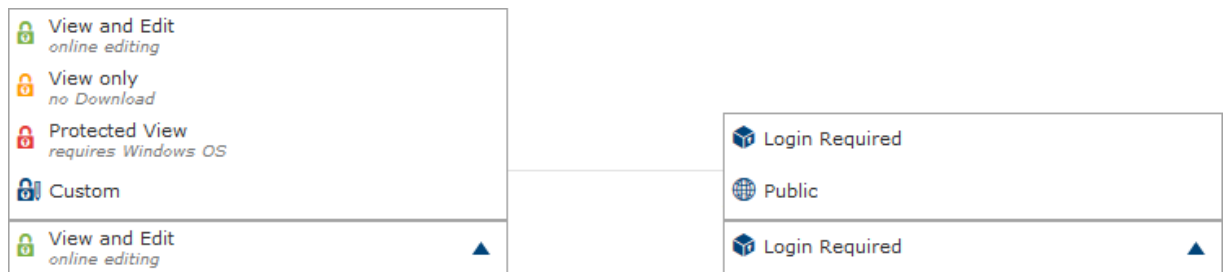
Within a work group, BooleBox guarantees optimum protection of shared data, with default file

classification according to encryption rules and access authorization established by the administrator. Each new file created and shared within the work group will automatically be given the level of protection set for its category and can be accessed only by users authorized according to pre-set rules.

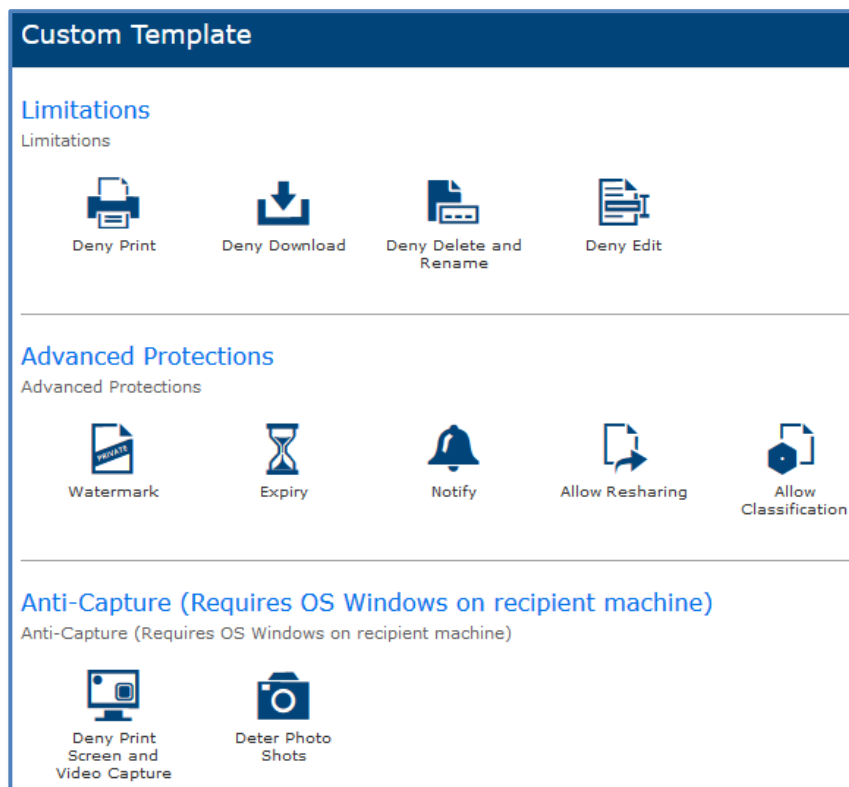
Thanks to the classification function, users decide not only WHO, but also HOW data can be accessed. BooleBox is designed to simplify file-sharing within a work group, without compromising the level of security. In addition to creating differentiated roles to be allocated to individual users, through the dashboard the administrator can also manage different categories of protection (with or without Personal Keys) for different data. Each file uploaded and shared is protected automatically, by specifying its category via a simple tag.

BooleBox users can access protected information from anywhere and at any time without the risk of reducing the security of their information. The congruity between a user requiring a specific operation on a file and the permissions he is granted for is checked by BooleBox for each operation required.

Security and Access control setting on uploaded data, can be configured choosing one of the following options:



or defining a custom template, selecting the following options:



- [23] **Privacy**
BBOP ensures its users total privacy, by storing their personal information in encrypted format: e-mail address, phone number, account credentials, by granting pseudonymity through aliases definition.
- [24] **Deny Download**
BooleBox users can enable the “Deny Download” function on documents they share online, to make them viewable and editable only in their BooleBox storage.
- [25] **Watermark**
With BooleBox users can protect their confidential documents and the intellectual property of their shared files through an indelible watermark displaying key information.
- [26] **Expiration**
BooleBox allows users to protect their data so that files can be accessed only until a given expiration date or within a specific time frame (minutes, hours, days), after which they will be inaccessible, even if they have been already accessed.
- [27] **Activity Logs**
BooleBox ’s advanced Auditing system ensures complete knowledge of all activity within the system. An administrator can see a clear visual report (Activity Log) of all the activities that have been carried out on a given file and track which operations have been performed by any given user. The Activity Logs, protected by encryption, can be accessed by BooleBox users through any browser and provide an advanced auditing system which contains detailed information about files setting history, WHO has accessed their data, WHAT operations have been performed, WHEN and WHERE (from which IP).
- [28] **Uploaded data versioning**
BooleBox file versioning ensures that every editing activity on a file generates a history where users can find the previously modified versions as well as keep on hand the latest updated version of your document.
- [29] Other non-security related functionalities offered by the TOE are:
- **Tagging**
BooleBox allows users to sort and manage their documents in an easy and organized way, without losing time in endless searches through their files.
 - **Annotations**
With BooleBox users can add and remove notes and annotations – both graphic and textual – on your documents and view all those created by other users.

1.5.3. TOE TYPE

[30] BooleBox On Premises V 4.2 is a software TOE, developed with Visual Studio 2013, can be viewed as covering to the following categories

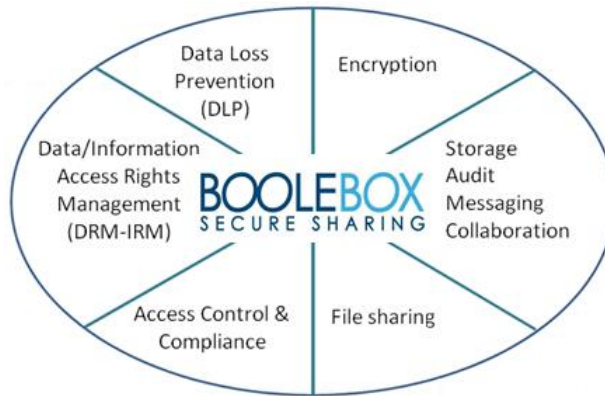


Figure 4: Product categories covered by BooleBox

[31] The TOE is represented below, in **BOLD**, in its operational environment:

End User side:

WEB BROWSER SUPPORTING HTML 5.0
OPERATING SYSTEM



Server side:

BOOLEBOX ON PREMISES V. 4.2
DBMS
.NET FRAMEWORK
IIS + SMS gateway + SMTP server
OPERATING SYSTEM

1.5.4. REQUIRED NON-TOE COMPONENTS

1.5.4.1. SERVER SIDE

Operating System (OS)	Microsoft Windows Server 2016 CC Certified for General Purpose Operating Systems Protection Profile compliancy (GP OS PP).
Minimum Software Prerequisites	Oracle MYSQL v. 5.7.22 (ENTERPRISE EDITION or MYSQL CLUSTER CARRIER GRADE EDITION or MYSQL COMMUNITY EDITION)
	Microsoft .NET Framework 4.8
	Microsoft IIS (Internet Information Services) 7.5 + SMS Gateway + SMTP Server
	N. 2 2048 bit RSA certificates
	BooleBox Storage Service, BooleBox Server Service, BooleBox Document Service.
Minimum Hardware Prerequisites¹	Ram: 8 GB or more
	Free Disk Space: 40 GB or more
	Network Card: 10/1000 Mbit or more
	CPU: Dual Core Processor
	Storage with NTFS partition and sufficient space for operational needs

Table 4: Minimum SW and HW prerequisites – server side

1.5.4.2. END USER SIDE

Operating System (required for Anti-Capture & Deter Photo Shots features)	Following versions of Microsoft Windows OS: <ul style="list-style-type: none"> • Microsoft Windows 10 • Microsoft Windows 8 e 8.1 • Windows 7
Software Prerequisites	Microsoft Internet Explorer (from version 10 and up) All other major internet browser (Chrome, Safari, Opera, Firefox) <i>Note:</i> Browsers HTML 5 compliant in their most updated version recommended.
Hardware Prerequisites	PC with at least the minimum hardware required by the operating system or in the event that Anti-Capture & Deter Photo Shots features are not required simply any fixed or mobile device on which an HTML 5 compatible web browser is installed.

Table 5: Software prerequisites – end user side

¹ *The hardware prerequisites indicated are recommended and not binding: the installation of the platform will therefore be possible even if the hardware available does not meet the minimum requirements indicated; in this case, however, performance problems could arise that do not affect the TOE security objectives of the operating environment anyway.*

1.6. TOE DESCRIPTION

- [32] Using BooleBox it is possible to create a Secure Cloud within an organization over the TLS 1.2 communication protocol.
- [33] BooleBox On premises 4.2 is installed in customer's infrastructure to centrally manage all system configurations for the infrastructure in which it is located BooleBox from the control panel available.
- [34] BooleBox is revolutionizing the secure sharing of confidential data, not only making it possible to individually select who the information is shared with, but also to enforce different access rights to multiple users of a single document.
BooleBox 's Granular and Dynamic Rights Management, based on classification templates, allows real time editing of any user's rights at any time. Access to information can be instantly revoked even after information has been shared.
File security is granted at all stages - "in motion" as well as "at rest": Secured files can be shared via the end user Clients or emailed to the recipient as a link to the shared file. Once shared, the correct file access policy is applied according to the latest version; ensuring appropriate access is always maintained.
- [35] The selected data managers can control their information and set sharing and access permissions:
- The protected File can be controlled for appropriate usage independent of its location.
 - The access rights to the file ensure that usage of the information is always in compliance with the latest company security policies.
 - Access rights are applied real-time – i.e. they can be changed after the distribution of the file. The "data owner" can change WHO/WHAT/WHEN/WHERE without requesting or resending the information to the recipients.

Although TOE authorized administrators can change the ownership of files, the use of this functionality, i.e. "Change Ownership", shall be limited to cases where access to company documents is required during prolonged absence of personnel or in the event of employee's resignation.

- [36] The TOE protects sensitive information from being disclosed through various channels, including email, print, or copy to an external storage device. Protection Rules link actions with definitions, tags and content categories, and rights assigned to user groups.
- [37] Protection rules (also according to classification templates) are applied each time an action on an upload file is attempted and this event, either successful or unsuccessful, is logged by BooleBox. In case of massive downloads by a user BooleBox, in addition, sends an alert to each user that share those data.
- [38] With reference to art. 32 of *General Data Protection EU Regulation 2016/679* (GDPR) BooleBox with the support of its operational environment supports data protection in different ways:
- **[Art. 32 comma 1.a]** with the pseudonymisation and encryption of personal data: BBOP ensures its users total privacy, by storing their personal information in encrypted format.
 - **[Art. 32 comma 1.b]** ensuring the ongoing confidentiality, integrity, availability of uploaded data (uploaded files are encrypted and stored together information to check their integrity and file names in the storage are not correlated in anyway with the original ones)

- **[Art. 32 comma 1.d]** thanks to Common Criteria certificate maintenance process the effectiveness of technical and organizational measures for ensuring the security of the processing is periodically tested, assessed and CC EAL2+ (Augmented with ALC_FLR.2) evaluated.
- **[Art. 32 comma 2]** thanks to Common Criteria EAL2+ (Augmented with ALC_FLR.2) evaluation and certification process, BBOP supports organizations in assessing the appropriate level of security taking into account the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

[39] The TOE is composed of the software implementing the components listed below, which can be accessed from the dashboard by an administrator:

- [40] **Company:** to create/delete the company or companies to which users belong;
- [41] **Users:** to create/delete/modify users;
- [42] **Groups:** to create/delete groups of users;
- [43] **User settings:** to define the profile of a specific user;
- [44] **Sharing templates:** to define sharing templates;
- [45] **Auditing:** to view which kind of information has been logged for a user withUSR profile;
- [46] **Administration Roles:** to define the profile of a specific administrator;
- [47] **Administration Log:** to view which kind of information must be logged for an administrator profile;
- [48] **Classification:** to define a classification project to simplify the process of applying centralized security policies through which different functional permissions can be applied to certain types of classifications according to each user.

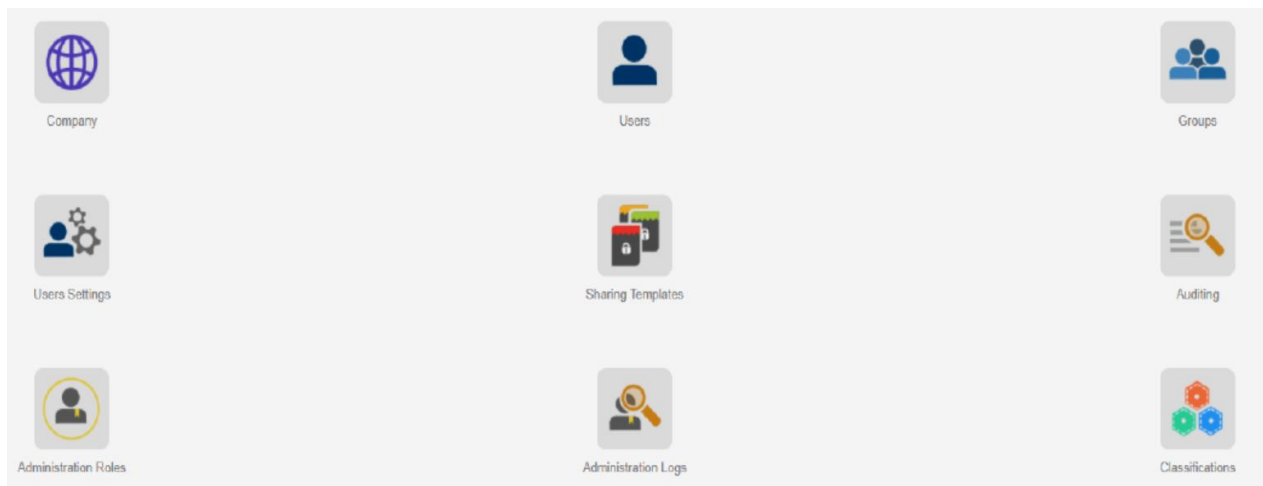


Figure 5: TOE components and Dashboard parameter settings

1.6.1. TOE USERS PROFILES

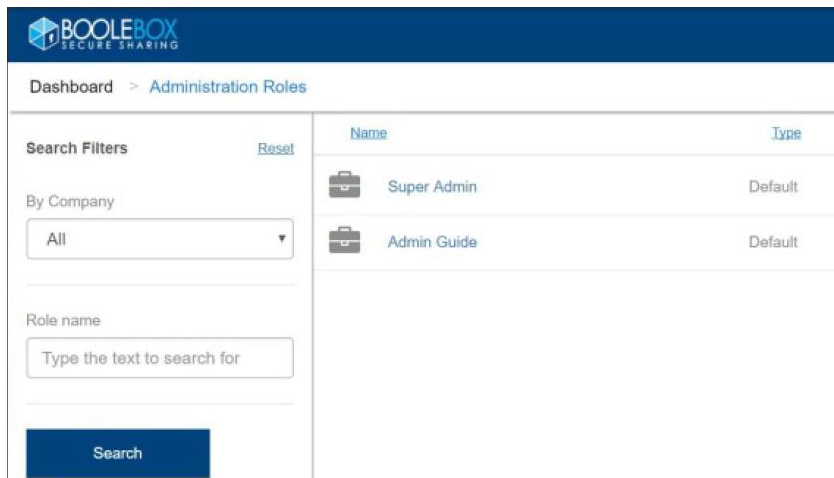
[49] This section shows the user profiles managed by BooleBox On Premises V 4.2. See SF_5 at § 7.1.5 for details on which operation are allowed for each user profile.

Administrative profiles:

- SUPER ADMIN (SAM),
- ADMIN (ADM),
- Administrative restricted roles (ADR)

The ADMINISTRATION ROLES section available in the BooleBox Dashboard includes two predefined profiles, created during BooleBox installation, SUPER ADMIN and ADMIN.

These administrative roles are assigned by default to the first user configured on the platform and cannot be edited or deleted.



Operative profiles:

- User (USR),
- Guest (GUEST).

1.6.2. PHYSICAL SCOPE OF THE TOE

[50] The TOE is a software TOE and it consists of the following software component:

- BooleBox On Premises Version 4.2.

[51] The customer obtains this software component, distributed with an .exe format, by accessing a shared folder made available by BooleServer Srl. For details, refer to the delivery procedures.

1.6.3. LOGICAL SCOPE OF THE TOE

[52] According to the description provided in §1.5.2, the logical boundary of the TOE includes the following type of security functionalities described in the following sections:

- Security Audit;
- Identification and authentication;
- Access Control
- User data protection
- TSF data protection
- Security Management

- Privacy

TSF	DESCRIPTION
Security Audit	<p>The solution includes an advanced auditing system that allows for complete and detailed track of any operations carried out on protected files, keeping the data owners and managers apprised of who views, modifies or shares protected files.</p> <p>Each operation performed by a USR role on a file and each operation performed by a SAM/ADM role has performed on a user profile is logged by BooleBox and can be audited according to auditing filters defined.</p> <p>Logs are stored encrypted in the DBMS.</p> <p>Logs can be viewed administrators by accessing the dashboard or by operative users by accessing their own work space.</p>
Identification and authentication	<p>The Identification and Authentication TSF ensures that only legitimate administrators can gain access to the configuration settings and management settings of the TOE.</p> <p>Each user must log in with a valid user name before the server will permit them to access the TOE.</p> <p>Due to the <i>two-step verification</i> setting, the TOE users must be strongly authenticated via an additional OTP password (unique code sent them via SMS that is different for each login attempt) before they can be granted to access stored data.</p> <p>Server-side users must log in with a valid user name and password before the server will permit the administrators to manage the TOE.</p>
Access control	<p>The TOE grants access to its functionalities only to authorized users, according to their profile.</p>
User data protection	<p>Using BooleBox, authorized users can work directly on the protected files, being able to share them with other users according to highly controlled policies: for example, a user may be authorized to read the content of certain files but without the ability to modify or to even save them locally, while another user can be granted read and write privileges, which may be granted for a limited time.</p>
Protection of the TSF	<p>The TOE with the support of its operational environment grants TSF data protection since it enforces requirements that the SFPs in the TOE cannot be tampered with or bypassed. TSF Data are protected both when exchanged with another trusted IT product (DBMS, OS or STORAGE) and at rest.</p>
Security Management	<p>The TOE provides a set of commands for authorized users to manage the security functions, configuration, and other features of the BooleBox. The Security Management function specifies user roles with defined access for the management of the TOE components.</p> <p>In general, the security data management function is made available to the owner of the data that want to share this information with other users.</p>
Privacy	<p>The TOE with the support of its operational environment grants users pseudonymity, i.e. granting that it's not possible to determine the real user name bound to specific operations performed by users, by providing an alias for the real name of users.</p>

1.6.4. TOE GUIDANCE DOCUMENTATION

- [53] The following guidance documentation is provided by Boole Server S.r.l., on demand, in PDF format as part of the TOE:
- [54] Users Guide: BooleBox online end user guide Version: 1 - Last update: 18th February 2020.
- [55] Administration Guide: "BooleBox online administrator guide Version: 1 - Last update: 18th February 2020"

1.6.5. USER DATA AND TSF DATA HANDLED BY THE TOE

- [56] The TOE handles the following TSF DATA:
- TOE MASTER KEY, generated at installation time and different for each BBOP instance,
 - TOE configurations {dashboard parameter settings as company configurations, users setting, etc.},
 - TOE Users' credentials,
 - AUDIT LOGs,
 - Sharing templates,
 - SHA-256 hash of uploaded data (USER DATA).
- [57] The TOE handles the following USER DATA:
- Personal information related to user account,
 - Uploaded data,
 - Email messages, when requested,
 - Classification projects.

2 CONFORMANCE CLAIM

2.1. CC CONFORMANCE CLAIM

- [58] This Security Target and this TOE conform to Common Criteria version 3.1 rev. 5.
- [59] This Security Target is compliant with:
- Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, conformant , ver. 3.1 Revision 5, April 2017, CCMB-2017-04-002
 - Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, conformant, ver. 3.1 Revision 5, April 2017, cod. CCMB-2017-04-003 at Evaluation Assurance Level 2 augmented with ALC_FLR.2.

2.2. PP CONFORMANCE CLAIM

- [60] This Security Target does not claim conformance to a Protection Profile.

3 SECURITY PROBLEM DEFINITION

- [61] This section describes the security aspects of the environment in which the TOE will be used and the way the TOE is expected to be employed.
- [62] To clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
 - Any organizational security policy statements or rules with which the TOE must comply.
 - Any assumptions about the security aspects of the environment and/or of the way the TOE is intended to be used.
- [63] This chapter identifies assumptions as A.ASSUMPTION, threats as T.THREAT and policies as P.POLICY.

3.1. THREATS

[64] The following table lists the threats.

[65] The assumed level of expertise of the attacker for all the threats is *basic*.

<i>Threat</i>	<i>Description</i>
T.MASQUERADE	A malicious external IT or human entity may obtain valid identification and authentication (I&A) data in order to masquerade as a legitimate user of the TOE.
T.INTERCEPT	A malicious external IT or human entity may intercept the data exchanged between a remote user and the TOE by sniffing the communication channel.
T.CONFIG	An unauthorized user may change the TOE configuration, intentionally or not, causing potential intrusions to go undetected.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.INTEGRITY	An unauthorized user may compromise the integrity of the data generated or stored by the TOE bypassing a security mechanism.
T.CONFIDENTIALITY	An unauthorized user may compromise the confidentiality of the configuration data and other data generated or stored by the TOE.
T.SCREEN	An unauthorized user may steal reserved data by taking a screen shot or taking a picture of the data viewed on the monitor.
T.NOTRACE	An unauthorized user may perform file operations or changes to TSF setting bypassing or disabling the audit functions, i.e. without being accountable for it.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.INTERR	A system failure or system crash makes unusable the current installation of the TOE or an unexpected interruption to the operation of the TOE or may cause security related data, such as audit data, to be lost or corrupted. Such interruptions may arise from human error or from failures of software, hardware, power supplies, or storage media.
T.EXHAUST	An attacker may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity.
T.KEY_ACCESS	A user or process may cause key (personal key or cryptographic key) to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.KEY_GUESS	An unauthorized user succeeds in guessing personal key or cryptographic keys due to weak keys.
T.INSTALL	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.REPLAY	A malicious external IT or human entity can access the TOE by replaying the authentication data of an authorized user.
T.PRIVACY	A malicious external IT or human entity can correlate a specific operation to the name of the TOE users who perform it.

Table 6: Threats

[112] The Threats reported in Table 6 may represent a risk for the following **TOE and non-TOE assets**:

- Personal information of TOE users;
- I&A data of both TOE administrators and TOE users;
- data exchanged between TOE “end user-side” and “Server-side”;
- stored TOE user data;
- stored TOE configuration data;
- stored TOE security functions and data;
- TSF settings;
- TOE applications normal (or expected) operation.

3.2. ORGANISATIONAL SECURITY POLICIES

[66] An organizational security policy is a set of rules, practices, and procedures intended to be imposed by an organization using Boole Box to address its security needs. This section of the security problem definition shows the OSPs that are to be enforced by the TOE, its operational environment, or a combination of the two.

<i>Policy</i>	<i>Description</i>
P.ACCOUNT	TOE Users shall be accountable for all their security related activities and for operations performed on a given file.
P.PROTECT	The TOE shall be protected from unauthorized access to its functions and data.
P.MANAGE	The TOE shall be managed only by authorized users.
P.ACCESS	Security related data collected and produced by the TOE shall only be used for authorized purposes by authorized users.
P.INTEGRITY	Security related data collected and produced by the TOE shall be protected from unauthorized modification.
P.PHYSICAL_ACCESS	The physical access to the area where the TOE is hosted shall be protected from unauthorized access.
P.CONFIGURATION	Authorized administrators are responsible for the correct configuration of both the TOE and its Operational Environment.
P.FAILURE	Those responsible for the TOE must ensure that procedures are in place to ensure that, after failures or other discontinuities affecting TOE operation, recovery without security compromise is obtained.
P.AUDITLOG	Authorized administrators must ensure that audit functions are used and managed effectively. These procedures shall apply to the TOE's audit trail and the audit trail for the underlying operating system. In particular: <ul style="list-style-type: none"> a) Appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs before audit trail exhaustion to ensure sufficient free space; b) Audit logs must be inspected on a regular basis and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future; c) The system clocks must be protected from unauthorized modification (so that the integrity of audit timestamps is not compromised).

Table 7: Organizational Security Policies

3.3. ASSUMPTIONS

[67] This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

<i>Assumption</i>	<i>Description</i>
A.TRUST	<p>It is assumed that the authorized administrators are not hostile, careless or willfully negligent observing the instructions provided by the TOE guidance documentation and in particular do not use the "Functional Account" functionality and use the "Change Ownership" functionality only when access to company documents is required during prolonged absence of personnel or in the event of employee's resignation.</p> <p>It is assumed that authorized administrators do not actively or negligently compromise the security of the server on which the TOE is installed. Examples for such compromising actions would be:</p> <ul style="list-style-type: none"> - Placing malicious software (like programs containing viruses or Trojan horses) on the server, - modifying the TOE program or data files.
A.TRAINING	It is assumed that users of the TOE will be trained sufficiently in order to properly configure, administrate, manage and operate the TOE.
A.DBMS_ACCESS	It is assumed that access to the database, used by the TOE via mechanisms outside the TOE boundary, is allowed only to authorized administrative users which are coordinated by the administrator of the TOE.
A.OS_ACCESS	<p>It is assumed that access to the Operating System, used by the TOE via mechanisms outside the TOE boundary, is allowed only to authorized administrative users which are also administrator of the TOE.</p> <p>Only TOE authorized administrators, after identification and authentication by the OS, can start and execute TOE components and review the log files stored by the OS.</p>
A.STORAGE_ACCESS	It is assumed that access to the storage, used by the TOE via mechanisms outside the TOE boundary, is allowed only to authorized administrative users which are coordinated by the administrator of the TOE.
A.DOC_ACCESS	It is assumed that access to the Document Manager Server, used by the TOE via mechanisms outside the TOE boundary, is allowed only to authorized administrative users which are coordinated by the administrator of the TOE.
A.TIME	It is assumed that the operational environment provides a reliable time reference.
A.ALIGNEDBACKUPS	It is assumed that BB Server, DBMS and Storage in TOE environment are regularly backup in a way that grants that the backups are kept aligned.
A.SECCOMM	It is assumed that the IT environment supports the TOE providing a secure line of communication between the TOE (Server-side) and end users' browsers.
A.TOE_EVALUATED	The TOE is installed, configured, and managed in accordance with its evaluated configuration.
A.OS_RESTRICT	The OS upon which the TOE resides will be configured to restrict modification to TOE executables, the OS itself, configuration files, databases to only the authorized administrators.
A.UPDATE	It is assumed that the IT environment administrator(s) ensure that the platform on which the TOE is running on allows secure operation of the TOE. Once vulnerabilities of the platform are known, which are relevant for TOE operation, these must be removed (e.g. by installing corresponding hot fixes) or protected by appropriate external security measures.

<i>Assumption</i>	<i>Description</i>
A.CERTIFICATE	It is assumed that IT environment ensures that the certificate containing the Kpriv and the Kpub used for BBOP MASTER KEY encryption/decryption is kept in a safe place under control of a Super Administrator (SAM).

Table 8: Assumptions

4 SECURITY OBJECTIVE

[68] Security objectives are concise, abstract statements of the intended solution to the security problem definition (see § 3). The set of security objectives for the TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment, as well as providing a mapping of the objectives to the threats, OSPs, and assumptions included in the security problem definition. This mapping also provides rationale for how the threats, OSPs, and assumptions are effectively and fully addressed by the security objectives.

4.1. SECURITY OBJECTIVES FOR THE TOE

[69] The IT security objectives for the TOE are addressed below:

<i>TOE Objective</i>	<i>Description</i>
O.AUDIT	The TOE must: <ul style="list-style-type: none"> - record audit records upon data accesses and use of the TOE functions; - make available audit tools to assist authorized users in the review of audit data.
O.AUDIT_PROT	The TOE shall enforce the integrity and confidentiality protection of audit information generated by itself.
O.USER	The TOE grants that only authorized administrators are allowed to create, delete, activate and suspend TOE users, to configure them, limiting their access to TOE functionalities.
O.IDENTIFY	The TOE shall identify users prior to allowing access to its functions and data.
O.ANTI_BRUTE	The TOE shall take specified actions or disable the account of the user that attempts to guess a password with brute force or dictionary attack.
O.ACCESS	The TOE shall allow authorized users to access only to authorized TOE functions and data according to their access rights.
O.MANAGE	The TOE shall include a set of functions that allows the effective management of its functionality and data by authorized administrators.
O.CONFIDENTIAL	The TOE shall protect the confidentiality of the user data when displayed.
O.CRYPTO	The TOE shall enforce files encryption before storing them, according to the owner's user profile.
O.INTEGRITY	The TOE must ensure the integrity of all user and TSF data.
O.CONFIG	The TOE, during the installation, shall ensure the presence of the required software.
O.OTP	The TOE shall implement a mechanism for user's strong authentication based on a static password and on a One Time Password (OTP).

<i>TOE Objective</i>	<i>Description</i>
O.STRONG_PERSONALKEY	The TOE accepts only personal keys satisfying the same complexity criteria as defined for users' passwords
O.PRIVACY	The TOE grants TOE users pseudonymity of the name of TOE users to specific operations they performed using the functions provided by the TOE.

Table 9: Security Objectives for the TOE

4.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

- [70] The operational environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality.
- [71] In the following table are described a set of statements describing the goals that the operational environment should achieve.

<i>Operational Environment Objective</i>	<i>Description</i>
OE.IDENTIFY	The Operational Environment supports the TOE in identifying and authenticating the authorized Operating System Administrators, authorized DBMS Administrator and authorized Storage Administrator
OE.AUDIT_PROTECT	The operational environment shall provide the capability to protect the integrity of audit log files generated by the TOE
OE.PHYSICAL_ACCESS	The physical access to the area where the TOE is hosted will be granted to TOE authorized administrators only.
OE.DB	Those responsible for the TOE configuration and administration must ensure that access to the database via mechanisms outside the TOE boundary is restricted to TOE authorized administrators only, that will be configured in the DBMS as database administrators. The DB is considered by the TOE as a trusted IT Product.
OE.SO	Those responsible for the TOE configuration and administration must ensure that access to the Operating System via mechanisms outside the TOE boundary is restricted to TOE authorized administrators only, that will be configured in the Operating System as OS System Administrators. Only TOE authorized administrators, after identification and authentication, can start and execute TOE components and review the log files stored by the OS. The OS is considered by the TOE as trusted IT product.
OE.STORAGE	Those responsible for the TOE configuration and administration must ensure that physical and logical access to the storage in TOE environment via mechanisms outside the TOE boundary is restricted to TOE authorized administrative users only. The STORAGE is considered by the TOE as trusted IT product.
OE.DOC	Those responsible for the TOE configuration and administration must ensure that access to the Document Manager Server via mechanisms outside the TOE boundary is restricted to TOE authorized administrators only, that will be configured in the Document Manager Server as Document Manager Server Administrators. The Document Manager Server is considered by the TOE as a trusted IT Product.

<i>Operational Environment Objective</i>	<i>Description</i>
OE.STAFF	<p>Staff working as TOE authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE and proper TOE configuration at installation phase.</p> <p>TOE authorized administrators configure and use the TOE observing the instructions provided by the TOE guidance documentation and in particular do not use the “Functional Account” functionality and use the “Change Ownership” functionality only when access to company documents is required during prolonged absence of personnel or in the event of employee's resignation.</p>
OE.TIME	The operational environment shall provide a reliable time reference.
OE.CRYPTO	The Operational Environment shall provide FIPS 140-2 validated cryptographic functionalities (RSA 2048 bit key generation, AES 256 bit key generation, Random Number Generation for OTP generation, Random alphanumeric string generation for key generation, RSA encryption/decryption, SHA256 hashing, AES 256 encryption/decryption using .NET 4.8 libraries) and protocols (HTTPS based on AES 256 and RSA 2048) to properly support the TOE for audit log file protections and secure transfer of information between End User side and Server Side and between the TOE and other non-TOE component required in the TOE environment.
OE.ALIGNEDBACKUP	The operational environment shall provide a secure back-up of DBMS and Storage data and the BooleBox.dat file and Activation Certificate used to encrypt the master key
OE.CONTINUITY	The operational environment shall provide a system to ensure operational continuity in the event of a power failure.
OE.AUDIT	The Operational Environment shall support the TOE in the generation of audit records, correlating them to the proper user when applicable, as a result of specific TOE activities and operations performed by TOE users. In addition, the Operational Environment shall guarantee that only OS System Administrators (the only System Administrators configured at OS level are TOE authorized administrators) can accede and visualize the aforementioned audit information.
OE.LOG_STORE	The operating environment shall grant that there is enough space dedicated to log management
OE.INTEGRITY	The Operational environment shall provide the capability to protect the integrity of executable files of the TOE using .NET framework technology.
OE.CERTIFICATE	The Operational environment shall support the TOE generating and securely storing the certificate containing the K_{priv} and the K_{pub} used for BBOP MASTER KEY encryption/decryption.
OE.PERSONALKEY	The Operation environment shall grant a secure distribution of a personal key correlate to a classification project and users are responsible for the secure management of their personal keys.

Table 10: Security objectives for the operational environment

4.3. SECURITY OBJECTIVES RATIONALE

[72] This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high-level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE THREAT POLICIES ASSUMPTION	OBJECTIVE														POLICY																			
	O.AUDIT	O.AUDI_PROT	O.USER	O.IDENTIFY	O.ANTI_BRUTE	O.ACCESS	O.MANAGE	O.CONFIDENTIAL	O.CRYPTO	O.INTEGRITY	O.CONFIG	O.OTP	O.STRONG_PERSONALKEY	O.PRIVACY	OE.IDENTIFY	OE.AUDIT_PROTECT	OE.PHYSICAL_ACCESS	OE.DB	OE.SO	OE.STORAGE	OE.DOC	OE.STAFF	OE.TIME	OE.CRYPTO	OE.ALIGNEDBACKUP	OE.CONTINUITY	OE.AUDIT	OE.LOG_STORE	OE.INTEGRITY	OE.CERTIFICATE	OE.PERSONALKEY			
T.MASQUERADE																																		
T.INTERCEPT																																		
T.CONFIG																																		
T.PRIVIL																																		
T.INTEGRITY																																		
T.CONFIDENTIALITY																																		
T.SCREEN																																		
T.NOTRACE																																		
T.LOSSOF																																		
T.INTERR																																		
T.EXHAUST																																		
T.KEY_ACCESS																																		
T.KEY_GUESS																																		
T.INSTALL																																		
T.REPLAY																																		
T.PRIVACY																																		
P.ACCOUNT																																		
P.PROTECT																																		
P.MANAGE																																		
P.ACCESS																																		
P.INTEGRITY																																		
P.PHYSICAL_ACCESS																																		
P.CONFIGURATION																																		
P.FAILURE																																		
P.AUDITLOG																																		

OBJECTIVE THREAT POLICIES ASSUMPTION	O.AUDIT	O.AUDI_PROT	O.USER	O.IDENTIFY	O.ANTI_BRUTE	O.ACCESS	O.MANAGE	O.CONFIDENTIAL	O.CRYPTO	O.INTEGRITY	O.CONFIG	O.OTP	O.STRONG_PERSONALKEY	O.PRIVACY	OE.IDENTIFY	OE.AUDIT_PROTECT	OE.PHYSICAL_ACCESS	OE.DB	OE.SO	OE.STORAGE	OE.DOC	OE.STAFF	OE.TIME	OE.CRYPTO	OE.ALIGNEDBACKUP	OE.CONTINUITY	OE.AUDIT	OE.LOG_STORE	OE.INTEGRITY	OE.CERTIFICATE	OE.PERSONALKEY		
	A.TRUST																																
A.TRAINING																																	
A.DBMS_ACCESS																																	
A.OS_ACCESS																																	
A.STORAGE_ACCESS																																	
A.DOC_ACCESS																																	
A.TIME																																	
A.ALIGNEDBACKUP																																	
S																																	
A.SECCOMM																																	
A.TOE_EVALUATED																																	
A.OS_RESTRICT																																	
A.UPDATE																																	
A.CERTIFICATE																																	

Table 11: Tracing between security objectives for the TOE and security objectives for the Operational Environment vs Threat, OSP and Assumption

[73] The following table provides detailed evidence of coverage for each threat, policy, and assumption

THREAT, POLICIES, ASSUMPTION	
T.MASQUERADE	<p>A threat agent masquerading as the TOE may capture valid identification and authentication data for a legitimate administrator of the TOE in order to gain unauthorized access to the TOE.</p> <p>The O.ANTI_BRUTE grants that the TOE is able to recognize and react disabling the account of a user who is trying to guess a password with brute force or dictionary attack.</p> <p>The O.OTP requires that the TOE shall implement a mechanism for authentication based on One Time Password (OTP) which send the OTP to BBOP user via a predefined cell phone number.</p> <p>The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit.</p>
T.INTERCEPT	<p>A malicious external IT or human entity may intercept the data exchanged between a remote user and the TOE by sniffing the communication channel.</p> <p>The O.CRYPTO objective states that the TOE encrypts the files before storing them, according to the owner's user profile.</p> <p>The OE.CRYPTO provides cryptographic functionality and protocols required for the TOE to properly support the TOE for secure transfer of information between End User side and Server side and between the TOE and other non-TOE component required in the TOE environment.</p>
T.CONFIG	<p>An unauthorized user may change the configuration of the TOE, intentionally or not, causing potential intrusions to go undetected.</p> <p>The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective only permit authorized users to access TOE functions. Besides, O.MANAGE provides a set of functions that allows the effective management of TOE functionality and data by authorized users.</p>
T. PRIVIL	<p>An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.</p> <p>The O.USER objective grants that only authorized administrators are allowed to create/delete/configure/limit the access to TOE functions to USR users.</p> <p>Authorized Administrators are faithfully selected (OE.STAFF)</p> <p>The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective only permit authorized users to access TOE functions.</p> <p>The O.ANTI_BRUTE grants that the TOE is able to recognize and react disabling the account of a user who is trying to guess a password with brute force or dictionary attack.</p>
T.INTEGRITY	<p>An unauthorized user may compromise the integrity of the data generated or stored by the TOE by bypassing a security mechanism.</p> <p>The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective only permits authorized users to access TOE data.</p> <p>The O.INTEGRITY objective ensures the TOE preserves data integrity. O.AUDIT_PROT/OE.AUDIT_PROTECT specifically refer to audit data integrity grant by the TOE together with its environment.</p> <p>The O.CRYPTO objective grants the TOE encrypts file before storing them.</p>

THREAT, POLICIES, ASSUMPTION	
	<p>The OE.CERTIFICATE objectives grants that the TOE operational environment supports the TOE generating and securely storing the certificate containing the K_{priv} and the K_{pub} used for BBOP MASTER KEY encryption/decryption.</p> <p>The O.ANTI_BRUTE grants that the TOE is able to recognize and react disabling the account of a user who is trying to guess a password with brute force or dictionary attack.</p>
T.CONFIDENTIALITY	<p>An unauthorized user may compromise the confidentiality of the configuration data and other data generated or stored by the TOE.</p> <p>The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective only permits authorized users to access TOE data.</p> <p>The O.CRYPTO objective grants the TOE encrypts file before storing them.</p> <p>The OE.CERTIFICATE objectives grants that the TOE operational environment supports the TOE generating and securely storing the certificate containing the K_{priv} and the K_{pub} used for BBOP MASTER KEY encryption/decryption.</p>
T.SCREEN	<p>An unauthorized user may stole reserved data by taking a screen shot or taking a picture of the data viewed on the monitor.</p> <p>O.CONFIDENTIAL protects the confidentiality of the user data when displayed.</p>
T.NOTRACE	<p>An unauthorized user may perform file operations bypassing or disabling the audit functions, i.e. without being accountable for it.</p> <p>The O.IDENTIFY objective provides for identification of users prior to any TOE data access, while OE.IDENTIFY grants the support by TOE operational environment to the TOE in identifying and authenticating OS and DBMS administrators Note that OE.PHYSICAL_ACCESS grants that only TOE authorized administrators are granted the access to the area where the TOE is hosted.</p> <p>The O.ACCESS objective only permit authorized users to access TOE functions.</p> <p>The O.AUDIT/OE.AUDIT objectives requires auditing of all data accesses and use of TOE functions; the operational environment supports the TOE in audit data generations. OE.TIME requires that the TOE Environment provide reliable time reference to be used in the audit logs. This helps prevent threat agents from performing security-relevant actions without being held accountable.</p> <p>OE.AUDIT_PROTECT requires that the TOE Environment store logs captured by the TOE of management operations performed on the TOE and encrypted by the TOE. This prevents threat agents from performing security-relevant actions without detection.</p> <p>O.AUDIT_PROT requires that the TOE protects log records confidentiality and integrity.</p>
T.LOSSOF	<p>An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.</p> <p>The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective only permit authorized users to access TOE functions. The O.INTEGRITY objective ensures no TOE data will be deleted.</p> <p>The OE.DB/OE.SO/OE.STORAGE grants that the OS/DB/STORAGE are configured and managed by TOE administrators.</p> <p>The OE.STAFF objective ensures competent administrators will manage the TOE.</p>
T.INTERR	<p>Unexpected interruptions to the operation of the TOE may cause security related data, such as audit data, to be lost or corrupted. Such interruptions may arise from human error or from software, hardware, power supplies or storage media failures.</p> <p>OE.CONTINUITY requires that the TOE Environment provides a system to ensure operational continuity in the event of power failure.</p> <p>OE.ALIGNEDBACKUP requires that the TOE Environment provide a secure back-up of DBMS and storage data and the BooleBox.dat file and Activation Certificate used to encrypt the master key.</p> <p>The OE.STAFF objective ensures competent administrators will manage the TOE.</p>

THREAT, POLICIES, ASSUMPTION

T.EXHAUST	<p>An attacker may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity.</p> <p>The OE.LOG_STORE grants the Operational Environment supports to the TOE in granting enough space for log management.</p> <p>The OE.STAFF objective ensures competent administrators will manage the TOE.</p>
T.KEY_ACCESS	<p>A user or process may cause key (personal key or cryptographic key) to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.</p> <p>The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The O.ACCESS objective only permit authorized users to access TOE functions.</p> <p>Anyway Personal Keys are never stored by the TOE. OE.IDENTIFY grants the support by TOE operational environment to the TOE in identifying and authenticating OS and DBMS administrators.</p> <p>Note that OE.PHYSICAL_ACCESS grants that only TOE authorized administrators are granted the access to the area where the TOE is hosted..</p> <p>The OE.DB (where the TOE MASTER KEY is stored)/OE.SO grants that the OS/DB are configured and managed by TOE administrators.</p> <p>The OE.STAFF objective ensures competent administrators will manage the TOE.</p>
T.KEY_GUESS	<p>An unauthorized user succeeds in guessing personal key or cryptographic keys due to weak keys.</p> <p>O.STRONG_PERSONALKEY grants that the TOE accepts only personal key defined by TOE users satisfying the same complexity criteria of TOE user passwords.</p> <p>Besides, according to OE.PERSONALKEY, the TOE operational environment grants a secure distribution of a personal key correlated to a classification project and users are responsible for the secure management of their personal keys (which are not stored by the TOE).</p> <p>The O.PRIVACY grants TOE users pseudonimity of the name of TOE users to specific operations they performed using the functions provided by the TOE.</p>
T.INSTALL	<p>An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.</p> <p>O.CONFIG objective ensures, during the installation, the presence of software required for the operativity.</p> <p>OE.STAFF objective ensures that the staff working as authorized administrator is faithfully selected, skilled and trained for proper operation without compromising the TOE.</p>
T.CRASH	<p>OE.BACKUP requires that the TOE Environment provide a secure back-up of DBMS and storage data.</p>
T.REPLAY	<p>A malicious external IT or human entity can access the TOE by replaying the authentication data of an authorized user .</p> <p>The O.ANTI_BRUTE grants that the TOE is able to recognize and react disabling the account of a user who is trying to guess a password with brute force or dictionary attack.</p> <p>The O.OTP requires that the TOE shall implement a mechanism for authentication based on One Time Password (OTP) which send the OTP to BBOP user via a predefined cell phone number.</p>
T.PRIVACY	<p>A malicious external IT or human entity can correlate a specific operation to the name of the TOE users who perform it.</p> <p>The O.PRIVACY grants TOE users pseudonimity of the name of TOE users to specific operations they performed using the functions provided by the TOE.</p> <p>The OE.STAFF objective ensures that the staff working as authorized administrator is faithfully selected, skilled and trained for proper</p>

THREAT, POLICIES, ASSUMPTION	
	configure the TOE according to TOE operational guides prescription.
P.ACCOUNT	<p>Users of the TOE shall be accountable for their activities and operations performed on a given file.</p> <p>The O.IDENTIFY objective supports this policy by ensuring each user is uniquely identified. OE.IDENTIFY grants the TOE operational environment supports the TOE in identifying OS/DBMS/STORAGE administrators.</p> <p>The O.AUDIT objective provides the ability for administrators to review the audit records generated by the TOE so that accountability for administrator actions can be determined.</p> <p>OE.TIME requires that the TOE Environment provide reliable time reference to be used in the audit logs.</p> <p>OE.AUDIT supports the TOE by generating in TOE operational environment audit records related to activities performed by OS/DBMS administrators (that are also TOE administrators).</p> <p>The OE.LOG_STORE grants the Operational Environment supports to the TOE in granting enough space for log management.</p> <p>The OE.INTEGRITY requires that operational environment provide the capability to protect the integrity of executable files of the TOE using .NET framework technology.</p>
P.PROTECT	<p>The TOE shall be protected from unauthorized access to its functions and data.</p> <p>The O.IDENTIFY objective provide users identification prior to any TOE data access.</p> <p>The O.ACCESS objective only permit authorized users to access TOE functions.</p> <p>The O.CRYPTO objective state that the TOE enforce encryption of the files and logs before storing them, according to the owner’s user profile.</p> <p>The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit.</p> <p>The OE.STORAGE objective requires the IT Environment to provide the TOE with TOE data storage and retrieval mechanisms.</p> <p>The OE.SO objective requires the Operational Environment to allow only TOE Authorized Administrators to start and execute TOE components and review the log files stored by the OS.</p> <p>O.AUDIT requires that the TOE capture logs of management operations performed on the TOE. This prevents threat agents from performing security-relevant actions without detection.</p> <p>O.AUDIT_PROT requires that the TOE enforces, with the support of TOE operational environment, integrity and confidentiality protection of audit records.</p>
P.MANAGE	<p>The TOE shall only be managed by authorized users.</p> <p>O.MANAGE foresees that the TOE includes a set of functions that allows the effective management of its functionality and data by authorized administrators.</p> <p>The OE.STAFF objective ensures competent administrators will manage the TOE.</p> <p>The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses. The O.ACCESS objective only permit authorized users to access TOE functions.</p>
P.ACCESS	Security related data collected and produced by the TOE shall only be used for authorized purposes by authorized users.

THREAT, POLICIES, ASSUMPTION	
	<p>The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses via the web interface. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions. The OE.DB/OE.SO/OE.STORAGE objective support this policy as those responsible for the TOE must ensure that access to the database/operating system/storage via mechanisms outside the TOE boundary is restricted to authorized administrative users only. The OE.STAFF objective ensures competent administrators will manage the TOE.</p>
P.INTEGRITY	<p>Security related data collected and produced by the TOE shall be protected from unauthorized modification.</p> <p>The O.INTEGRITY objective ensures the protection of TOE data from modification.</p> <p>The O.AUDIT_PROT/OE.AUDIT_PROTECT objective ensures the TOE enforces audit data encryption and the integrity of audit records in the database generated by the TOE using access mechanisms outside the TSF.</p> <p>The O.CRYPTO objective state that the TOE encrypts the files and logs before storing them, according to the owner’s user profile.</p> <p>The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit.</p> <p>The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses via the web interface.</p> <p>O.ACCESS objective supports this policy as the TOE shall allow authorized users to access only to authorized TOE functions and data.</p> <p>The OE.DB/OE.SO objectives support this policy as those responsible for the TOE must ensure that access to the database and the operating system via mechanisms outside the TOE boundary is restricted to authorized administrative users only.</p>
P.PHYSICAL_ACCESS	<p>The physical access to the area where the TOE is hosted shall be protected from unauthorized access.</p> <p>OE.PHYSICAL_ACCESS specify that the physical access to the area where the TOE is hosted will be granted to TOE authorized administrators only.</p>
P.CONFIGURATION	<p>Authorized administrators are responsible for the correct configuration of both the TOE and its Operational Environment.</p> <p>The OE.STAFF objective ensures competent administrators will manage the TOE.</p> <p>O.CONFIG ensures that the TOE grants the presence of all required software.</p>
P.FAILURE	<p>Those responsible for the TOE must ensure that procedures are in place to ensure that, after failures or other discontinuities affecting TOE operation, recovery without security compromise is obtained.</p> <p>OE.CONTINUITY ensures that the operational environment provides a system to ensure business continuity in the event of a power failure;</p> <p>OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE.</p> <p>OE.ALIGNEDBACKUP ensures that the operational environment provides a secure back-up of DBMS and Storage data and the BooleBox.dat file and Activation Certificate used to encrypt the master key.</p>
P.AUDITLOG	<p>OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE.</p> <p>OE.LOG_STORE requires that the TOE Environment grants, with adequate procedures to be applied by TOE administrators, that there is</p>

THREAT, POLICIES, ASSUMPTION

	<p>enough space for log management.</p> <p>OE.TIME requires that the TOE Environment provide reliable time reference to be used in the audit logs.</p>
A.TRUST	OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected for proper operation without compromising the TOE.
A.TRAINING	OE.STAFF ensures that personnel working as authorized administrator shall be skilled and trained for proper operation without compromising the TOE.
A.DBMS_ACCESS	The OE.DB objective ensures that physical and logical access to any mechanisms outside the TOE boundary that may be used to access the database is managed by the administrators which are also TOE administrator such that only authorized users may utilize the mechanisms.
A.OS_ACCESS	The OE.SO objective ensures that physical and logical access to any mechanisms outside the TOE boundary that may be used to access the OS is managed by the administrators which are also TOE administrator such that only authorized users may utilize the mechanisms.
A.STORAGE_ACCESS	The OE.STORAGE objective ensures that physical and logical access to any mechanisms outside the TOE boundary that may be used to access the storage is managed by the administrators which are also TOE administrator such that only authorized users may utilize the mechanisms.
A.DOC_ACCESS	The OE.DOC ensures that physical and logical access to any mechanisms outside the TOE boundary that may be used to access the Document Manager Server is managed by the administrators which are also TOE administrator such that only authorized users may utilize the mechanisms.
A.TIME	A.TIME assumption is upheld by OE.TIME objective requiring the operational environment to provide a reliable time reference.
A.ALIGNEDBACKUPS	OE.ALIGNEDBACKUP ensures that operational environment provides a secure backup of DBMS and storage data and the BooleBox.dat file and Activation Certificate used to encrypt the master key.
A.SECCOMM	OE.CRYPTO ensures that all communications between TOE components and between the TOE and remote users is protected.
A.TOE_EVALUATED	OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE.
A.OS_RESTRICT	<p>OE.SO grants that the OS administrators will be TOE Administrators.</p> <p>OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE. The OS upon which the TOE resides will be configured to restrict modification to TOE executables, the OS itself, configuration files, databases to only the authorized administrators.</p>
A.UPDATE	OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE.
A.CERTIFICATE	OE.CERTIFICATE grants that the TOE operational environment shall support the TOE generating and securely storing the certificate containing the K_{priv} and the K_{pub} used for BBOP MASTER KEY encryption/decryption.

Table 12: Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 EXTENDED COMPONENTS DEFINITION

5.1. EXTENDED COMPONENTS DEFINITION

[74] No extended Security Functional Requirements (SFRs) are defined for the TOE.

[75] No extended Security Assurance Requirements (SARs) are defined for the TOE.

6 SECURITY REQUIREMENTS

[76] In this section, the TOE security requirements are defined in terms of Security Functional Requirements (SFRs), specified according to conventions explained in section 1.4, and Security Assurance Requirement (SARs).

6.1. SECURITY FUNCTIONAL REQUIREMENTS

[77] The functional security requirements for this Security Target consist of the following components from Part 2 of the CC [CCP2]: all of which are summarized in the following table detailing the operations that have been performed on the SFRs.

		A	S	R	I
FAU - Security Audit					
FAU_GEN.1	Audit data generation	x	x		
FAU_GEN.2	User identity association				
FAU_SAR.1	Audit Review	x			x
FAU_SAR.2	Restricted Audit Review				
FAU_SAR.3	Selectable audit review	x			
FIA - Identification and authentication					
FIA_AFL.1	Authentication failure handling	x	x		
FIA_UID.2	User identification before any action				
FIA_UAU.2	User authentication before any action				
FIA_UAU.5	Multiple authentication mechanisms	x			
FIA_ATD.1	User attribute definition	x			
FIA_SOS.1	Verification of secrets	x		x	
FDP – User Data Protection					
FDP_ACC.1	Subset access control	x			x
FDP_ACF.1	Security attribute based access control	x			x
FDP_ITC.1	Import of user data without security attributes	x			
FDP_ITC.2	Import of user data with security attributes	x			
FDP_ETC.1	Export of user data without security attributes	x			
FDP_ETC.2	Export of user data with security attributes	x			
FDP_IFC.1	Subset information flow control	x			
FDP_IFF.1	Simple security attribute	x			
FDP_UCT.1	Basic data exchange confidentiality	x	x		
FDP_UIT.1	Data exchange integrity	x	x		

FPT – Protection of the TSF					
FPT_TDC.1	Inter-TSF basic TSF data consistency	x			
FPT_TEE.1	Testing of external entities	x	x		
FMT – Security management					
FMT_MTD.1	Management of TSF data	x	x		
FMT_MOF.1	Management of security functions behavior	x	x		
FMT_MSA.1	Management of security attributes	x	x		x
FMT_MSA.3	Static attribute initialization	x	x		x
FMT_SMF.1	Specification of Management Functions	x			x
FMT_SMR.1	Security Roles	x			
FPR – Privacy					
FPR_UNO.1	Unobservability	x			
FPR_PSE.1	Pseudonymity	x	x		

Table 13: List of SFR and related operations

[78] The rest of this section details the functional requirements taken from the catalog [CCP2], organized by functional families, and adapts them for this Security Target.

6.1.1. SECURITY AUDIT

[79] FAU_GEN SECURITY AUDIT DATA GENERATION

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 an audit record 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; and
- c) *auditable events defined in Table 30 and Table 31 of paragraph SF_2: Audit*

FAU_GEN.1.2

The TSF shall record within the 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, *IP address of End User's device*.

Application Note:

Since the audit function is always active, start-up and shutdown of the audit function is not being audited. The outcome (success or failure) of the events is not recorded: all events are registered when have success outcome. The Login with failure outcome is recorded as a "Login Failed" event.

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.

[80] FAU_SAR: SECURITY AUDIT REVIEW

FAU_SAR.1 (1) Audit review

FAU_SAR.1.1

The TSF shall provide *users with role SAM or ADM or ADR with permission to access the ADMINISTRATIVE LOGS section of the dashboard* with the capability to read *all audit information in Table 30 and in Table 31* 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.

FAU_SAR.1 (2) Audit review

FAU_SAR.1.1

The TSF shall provide *users with role USR and DASHBOARD.USER SETTINGS.SECTIONS VISIBILITY.ACTIVITY LOGS permission enabled by the*

authorized administrator who create the user with the capability to read *all audit information in Table 30 on the files he owns* 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.

FAU_SAR.2 Restricted audit review

FAU_SAR.2.1

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review

FAU_SAR.3.1

The TSF shall provide the ability to apply *searches* of audit data based on *Date of the event and/or type of event and/or subject identity*.

6.1.2. IDENTIFICATION AND AUTHENTICATION

[81] FIA_AFL: AUTHENTICATION FAILURES

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1

The TSF shall detect when *three (3)* unsuccessful authentication attempts occur related to *consecutive instance of a user attempting to authenticate themselves*.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall *require the user to insert a captcha code foreseeing an increasing delay for each wrong captcha code inserted*.

[82] FIA_UID: USER IDENTIFICATION

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.

Application note: The Identification of the TOE authorized administrators for the access to the Control Panel is delegated to the Operational Environment of the TOE (Operating System).

[83] FIA_UAU: USER AUTHENTICATION

FIA_UAU.2 User authentication before any action

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.5 Multiple authentication mechanisms

FIA_UAU.5.1

The TSF shall provide *static password, One Time Password (OTP)* to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the *following rule: first authentication step by static password and only if the first authentication step is successfully it is required to enter a OTP that is sent to the user via cell phone number*.

Application note: The OTP consists of at least 6 digits. The OTP expires after 5 minutes and each attempt to insert the correct OTP is subject to an increasing delay. The Guest user can access a shared file only after setting a static password without the need of OTP password. The authentication of the TOE authorized administrators for the access to the Control Panel is delegated to the Operational Environment of the TOE (Operating System).

[84] **FIA_ATD: USER ATTRIBUTE DEFINITION**

FIA_ATD.1 User attribute definition

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users:

- *User credentials (username, password, OTP)*
- *User type (internal/external),*
- *User status (active/inactive),*
- *User current access attempt*
- *User Role (SAM, ADM, ADR, USR, GUEST),*
- *(A specific) classification project membership*
- *User Privileges (See Table 14).*

Privileges	Description
SAM	SAM User has Super Administrator privileges as described in 6th column of Table 15
ADM	ADM User has Administrator privileges as described in 6 th column of Table 15
ADR	ADR User has restricted administrative privileges as defined by the authorized administrator who created it as described in 6 th column of Table 15
USR	User has USR privileges as described in 6 th column of Table 17
GUEST	GUEST User has the privilege to access files shared by TOE users with restricted permissions set in the sharing template associated to the file as described in Table 18

Table 14: User Privileges

Application note: for the Guest user the security attribute User credentials is only (username, password) without OTP.

[85] **FIA_SOS: SPECIFICATION OF SECRET**

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets (**PASSWORDS, PERSONAL KEYS**) meet

- *at least eight characters;*
- *at least one numeric character;*
- *at least one lowercase letter;*
- *at least one uppercase letter.*

6.1.3. USER DATA PROTECTION

[86] **FDP_ACC: ACCESS CONTROL POLICY**

FDP_ACC.1 (1) Subset access control

FDP_ACC.1.1

The TSF shall enforce the *BBOP Administrators access control SFP* on
Subjects: TOE user;
Objects: BBOP application;
Operations among subjects and objects covered by the SFP: as described in the sixth column of Table 15

FDP_ACC.1 (2) Subset access control

FDP_ACC.1.1

The TSF shall enforce the *BBOP Users access control SFP* on
Subjects: TOE user;
Objects: BBOP application;
Operations among subjects and objects covered by the SFP: as described in the sixth column of Table 16.

FDP_ACC.1 (3) Subset access control

FDP_ACC.1.1

The TSF shall enforce the *uploaded file access control SFP* on
Subjects: TOE user;
Objects: uploaded data;
Operations among subjects and objects covered by the SFP: as described in the sixth column of Table 17.

[87] **FDP_ACF ACCESS CONTROL FUNCTIONS**

FDP_ACF.1 (1) Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the *BBOP Administrators access control SFP* to objects based on the following: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes as specified in Table 15: BBOP Administrators access control SFP.*

SUBJECTS	SUBJECTS' ATTRIBUTES	RULES GOVERNING ACCESS AMONG CONTROLLED SUBJECTS AND CONTROLLED OBJECTS	OBJECTS	OBJECTS' ATTRIBUTES	ALLOWED OPERATIONS <i>The user shall access the functions offered by the OBJECT after providing a valid username and password. User privileges define operations the user can perform on the OBJECT.</i> ----- <i>see SF_4: Management for a detailed description of administration functionalities accessible from each Dashboard section</i>
TOE users	User's ROLE	User's role is SAM	BBOP Application	User privileges	The SAM TOE user has access to all TOE Operations allowed to ADM + permissions for creating new companies
		User's role is ADM	BBOP Application	User privileges	The ADM TOE user has the maximum permissions (i.e. FULL CONTROL) within a given company to access and use security

SUBJECTS	SUBJECTS' ATTRIBUTES	RULES GOVERNING ACCESS AMONG CONTROLLED SUBJECTS AND CONTROLLED OBJECTS	OBJECTS	OBJECTS' ATTRIBUTES	<p>ALLOWED OPERATIONS</p> <p><i>The user shall access the functions offered by the OBJECT after providing a valid username and password.</i></p> <p><i>User privileges define operations the user can perform on the OBJECT.</i></p> <p>-----</p> <p><i>see SF_4: Management for a detailed description of administration functionalities accessible from each Dashboard section</i></p>
					<p>relevant TOE functions offered by the dashboard:</p> <ul style="list-style-type: none"> • Administration roles • Users • User settings • Sharing templates • Auditing (including the setting of Users log period, i.e. the period in which all operations performed by any BooleBox end users are logged and stored encrypted in the database) • Administration Logs • Classifications
		User's role is ADR	BBOP Application	<p>User privileges as defined by a SAM/ADM user equal to:</p> <ul style="list-style-type: none"> • PERMISSION DENIED (i.e. NO PERMISSION), • READ ONLY permission, • MODIFY permissions for existing settings, • WRITE permissions for new settings, • FULL CONTROL. 	<p>The ADR TOE user is allowed to perform administrative task within a given company, according to permissions set by SAM/ADM or authorized ADR at its creation, to access and use security relevant TOE functions offered by the following sections of the dashboard:</p> <ul style="list-style-type: none"> • Administration roles • Users • User settings (Access Notification, Single Sign On, Personal Key, Custom sharing, External sharing, Public sharing, Sharing mode, Section Visibility, Sharing templates, Auditing, Administrative Logs, Classifications) • Sharing templates • Auditing (including the setting of Users log period, i.e. the period in which all operations performed by any BooleBox end users are logged and stored encrypted in the database) • Administration Logs • Classifications

Table 15: BBOP Administrators access control SFP

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects as specified in Table 15.*

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none.*

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none.*

Note: *USR and GUEST users do not have access to the Dashboard.*

FDP_ACF.1 (2) Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the *BBOP Users access control SFP* to objects based on the following: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes as specified in Table 16: BBOP Users access control SFP.*

SUBJECTS	SUBJECTS' ATTRIBUTES	RULES GOVERNING ACCESS AMONG CONTROLLED SUBJECTS AND CONTROLLED OBJECTS	OBJECTS	OBJECTS' ATTRIBUTES	ALLOWED OPERATIONS <i>The user shall access the functions offered by the OBJECT after providing a valid username and password. User privileges define operations the user can perform on the OBJECT</i> ----- <i>see SF_4: Management for a detailed description of each user setting with access to the USER SETTING section of the dashboard</i>
TOE users	User's ROLE	User's role is USR	BBOP Application	User privileges	<p>The USR has no access to any dashboard functions. The USR TOE user has restricted permissions within a given company to access and use the following TOE security functions according to the profile defined and assigned to the user when it was created by an authorized administrator with access to the USER SETTING section of the dashboard:</p> <ul style="list-style-type: none"> • Access Notification • Single Sign On • Personal Key • Custom sharing • External sharing • Public sharing • Sharing mode • Section Visibility <p>NOTE: Two step verification is not optional and is always required for each user</p>
TOE users	User's ROLE	User's role is GUEST	BBOP Application	User privileges	GUEST User has the privilege to access files shared by TOE users with restricted permissions set in the sharing template associated to the file as described in table 17.

Table 16: BBOP Users access control SFP

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects as specified in Table 16.*

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none.*

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none.*

FDP_ACF.1 (3) Security attribute based access control

FDP_ACF.1.1

The TSF shall enforce the *uploaded file access control SFP* to objects based on the following: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes as specified in Table 17: uploaded file access control SFP.*

SUBJECTS	SUBJECTS' ATTRIBUTES	RULES GOVERNING ACCESS AMONG CONTROLLED SUBJECTS AND CONTROLLED OBJECTS	OBJECTS	OBJECTS' ATTRIBUTES	ALLOWED OPERATIONS <i>The user shall access the functions offered by the OBJECT after providing a valid username and password. User privileges define operations the user can perform on the OBJECT</i>
TOE users	User's ROLE	User's role is SAM, ADM, ADR or USR AND user is the file.owner AND User is active	Uploaded file	file.owner	The user has full access to the file,
TOE users	User's ROLE	The TOE user is not the file.owner AND he has received a notification by email from the file owner that he will be able to access the file, according to its settings and respecting the security levels defined by the file owner AND User is active	Uploaded file	File.owner, File.Sharing template	The user to which the file has been shared has restricted permissions to access the shared file according to the sharing template associated to it. In table 17 are detailed the sharing permission that can be set by the owner of a file defining a specific sharing template. Note that the file owner can change the sharing permission on a previously shared file at any time and he is able to notify the recipient of the changes in any moment or to not notify anything at all.
TOE users	User's ROLE	The user is a member of the classification project, i.e. he belongs to the group of people to which the file is accessible according to the rules defined by one of the classification project administrators <input checked="" type="checkbox"/> AND User is active	Uploaded file	File.owner, File.SharingTemplate Classification project	the user (or users) defined as <i>members of the classification project</i> <input checked="" type="checkbox"/> can open the classified file in the manner set out in the classification project and according to the file.SharingTemplate specified in the classification project definition

Table 17: uploaded file access control SFP

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects as specified in Table 17.*

FDP_ACF.1.3

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *sending an email to the subject to which the file is shared by file owner.*

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *removing the email address from the list of subjects to which the file is shared.*

<p>Within each sharing Template, authorized TOE user can set one of the following LIMITATIONS that can be enabled or not:</p> <ul style="list-style-type: none"> • DENY UPLOAD - if enabled, this option does not allow the recipient of the share to upload to the folder that has been shared with them. • DENY PRINT - if activated, this option does not allow the recipient to print the shared content • DENY DOWNLOAD - if activated, this option denies the recipient the possibility to download files that have been shared with them. • DENY DELETE and RENAME - if activated, this option denies the recipient the possibility to delete or rename the resources that have been shared. • DENY EDIT - if activated, this option refuses the recipient the possibility to work on and modify the contents of a file.
<p>Within each sharing template, one of the following ADVANCED PROTECTION can be configured (enabled/disabled):</p> <ul style="list-style-type: none"> • WATERMARK - if activated, this option applies a watermark to the shared document; you can choose whether to apply it obliquely, or full screen. • EXPIRY - if activated, the option enables sharing for a limited period. By selecting DATE from the menu you can specify a date in the calendar beneath, beyond which the shared document will no longer be available to the recipient; by selecting PERIOD instead, it is possible to specify the validity period for sharing, in terms of minutes or hours (the duration of the validity set begins from the time the file is first opened by the recipient). • NOTIFY - if activated, this option sends an e-mail notification every time an operation is performed on the shared object. It is possible to select whether to send notifications ONLY ME, that is to say the user sharing the file or, if ALL RECIPIENT, to those who are part of the same share. • ALLOW RESHARING - if enabled, this option allows the recipient to share the received object in turn. • ALLOW CLASSIFICATION - if activated, this option allows the recipient to classify a file that has been shared with them.
<p>Within each sharing template, one of the following ANTI-CAPTURE options can be configured (enabled/disabled):</p> <ul style="list-style-type: none"> • DENY PRINT SCREEN AND VIDEO CAPTURE - if activated, this option does not allow screenshots to be made if the shared document is open. • DETER PHOTO SHOTS - if enabled, this option makes the document viewable in a limited mode, with just a small portion of the document visible at any time. • NOTE: The ANTI-CAPTURE options require that the recipient opens documents from a Windows operating system. Documents cannot be shared on any other OS.

Table 18: file sharing permissions configurable in a sharing template

[88] **FDP_IFC INFORMATION FLOW CONTROL POLICY**

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1

The TSF shall enforce the *BooleBox flow control SFP* on

Subjects: *TOE users, BBOP, DBMS, OS, Storage.*

Information: *user’s credentials (username, password), user personal information, uploaded data, encrypted uploaded data, email messages, sharing templates., TOE configurations, Audit Log.*

Operations: *user registration, user authentication, data upload (from TOE user to STORAGE), data download (from STORAGE to TOE user), encrypted email message sending, Audit Log Upload (from BBOP to DBMS), Audit Log Download (from DBMS to TOE user), TOE configuration update, sharing template update*

Application note:

The BooleBox flow control SFP is graphically depicted in the following figure.

Legenda:

“E-” means that data are encrypted

“C-” means that data are not encrypted

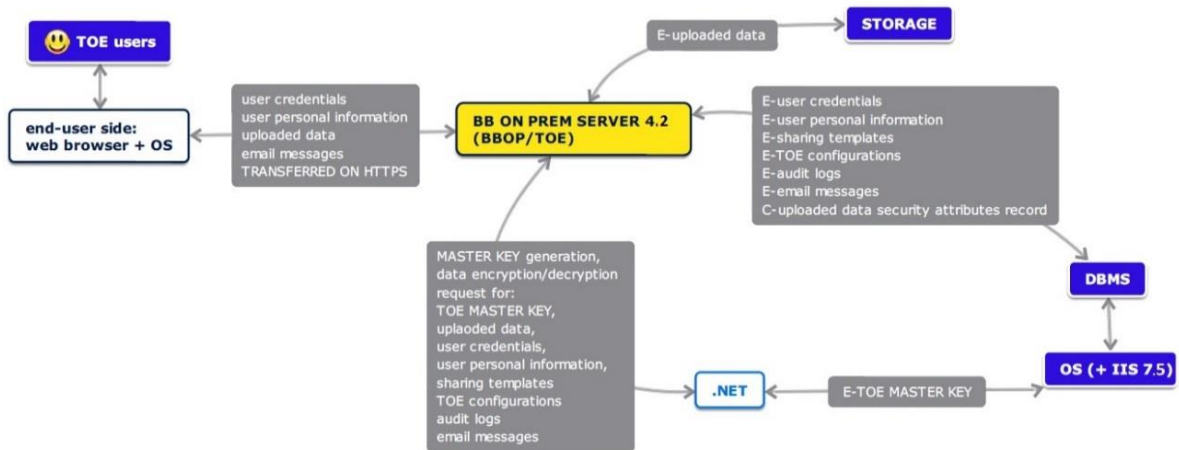


Figure 6: Boole Box flow control policy scheme

[89] **FDP_IFF INFORMATION FLOW CONTROL FUNCTIONS**

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1

The TSF shall enforce the *BooleBox flow control SFP* based on the following types of subject and information security attributes: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes as specified in Table 19.*

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes as specified in Table 19:*

SUBJECT	SECURITY ATTRIBUTE	POSSIBLE VALUE	
TOE users	credentials (username, password, OTP)	valid/invalid	
	type	internal/external	
	status	active/inactive	
	role	SAM, ADM, ADR, USR, GUEST	
	privileges	See details in Table 14, Table 15, Table 16 and Table 17	
BBOP Application	state	Ok/KO	
DBMS	state	Ok/KO	
OS	-	-	
STORAGE	state	Ok/KO	
INFORMATION	SECURITY ATTRIBUTE	POSSIBLE VALUE	
user's credentials (username, password)	status	encrypted / unencrypted	
user personal information	status	encrypted / unencrypted	
1024-byte block of uploaded data	status	encrypted / unencrypted	
uploaded data	personal key	null/not null	
email message	status	encrypted / unencrypted	
Audit Log	status	encrypted / unencrypted	
sharing template	status	encrypted / unencrypted	
TOE configurations	status	encrypted / unencrypted	
Encrypted uploaded data	filename	null / not null	
	file_ID (Unique identifier of the file in the Database)	null / not null	
	DBMS record	filename	valid/invalid
		File_ID (Unique identifier of the file in the Database)	null / not null
		Owner ID	correct/incorrect
		File size	correct/incorrect
File SHA-256 hash	correct/incorrect		
OPERATION	SECURITY ATTRIBUTE-BASED RELATIONSHIP BETWEEN SUBJECT SECURITY ATTRIBUTES AND INFORMATION SECURITY ATTRIBUTES		
user registration	The operation takes places if user personal information status = encrypted		
user authentication	The operation takes places if user's credentials (username, hashed password) status = encrypted		
data upload (from TOE user to STORAGE)	For each 1024-byte block of data to be uploaded the operation takes places if: Status of Owned file = encrypted		
data download (from STORAGE to TOE user)	The operation takes places if: <ul style="list-style-type: none"> - Owner Id (derived from the active session) = correct - File size = correct - File SHA-256 hash = correct - File_ID = not null - Filename = valid 		

OPERATION	SECURITY ATTRIBUTE-BASED RELATIONSHIP BETWEEN SUBJECT SECURITY ATTRIBUTES AND INFORMATION SECURITY ATTRIBUTES
encrypted email message sending	The operation takes places if email message status = encrypted
Audit Log Upload (from BBOP to DBMS)	The operation takes places if audit log status = encrypted
TOE configuration update	The operation takes places if TOE configuration status = encrypted
sharing template update	The operation takes places if sharing template status = encrypted

Table 19: BooleBox flow control SFP

FDP_IFF.1.3

The TSF shall enforce the *none*.

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: *none*.

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: *none*.

[90] FDP_ITC: IMPORT FROM OUTSIDE OF THE TOE**FDP_ITC.1 Import of user data without security attributes****FDP_ITC.1.1**

The TSF shall enforce the *BooleBox flow control SFP* when importing user data controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2

The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *none*.

Application note:

This requirement only applies to the following user data: USER PERSONAL INFORMATION, EMAIL MESSAGES.

FDP_ITC.2 Import of user data with security attributes**FDP_ITC.2.1**

The TSF shall enforce the *BooleBox flow control SFP* when importing user data controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2

The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3

The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4

The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: *rule named "Encrypted file integrity check"*

Note: The rules "Encrypted file integrity check" is detailed in § "7.1.3 SF_3: USER and TSF data protection" (Figure 9: file decryption process)

Application note: This requirement only applies to the following user data: UPLOADED DATA.

[91] **FDP_ETC: EXPORT FROM THE TOE**

FDP_ETC.1 Export of user data without security attributes

FDP_ETC.1.1

The TSF shall enforce the *BooleBox flow control SFP* when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2

The TSF shall export the user data without the user data's associated security attributes

Application note:

This requirement only applies to the following user data: USER PERSONAL INFORMATION, EMAIL MESSAGES

FDP_ETC.2 Export of user data with security attributes

FDP_ETC.2.1

The TSF shall enforce the *BooleBox flow control SFP* when exporting user data controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2

The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3

The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4

The TSF shall enforce the following rules when user data is exported from the TOE: *rule named "Encrypted file integrity check"*.

Note: The rules "Encrypted file integrity check" is detailed in § "7.1.3 SF_3: USER and TSF data protection" (Figure 8: file encryption process)

Application note:

This requirement only applies to the following user data: UPLOADED DATA

[92] **FDP_UCT: INTER-TSF USER DATA CONFIDENTIALITY TRANSFER PROTECTION**

FDP_UCT.1 Basic data exchange confidentiality

FDP_UCT.1.1

The TSF shall enforce the *BooleBox flow control SFP* to *transmit, receive* user data in a manner protected from unauthorized disclosure.

[93] **FDP_UIT: INTER-TSF USER DATA INTEGRITY TRANSFER PROTECTION**

FDP_UIT.1 Data exchange integrity

FDP_UIT.1.1

The TSF shall enforce the *uploaded file access control SFP and BooleBox flow control SFP* to *transmit, receive* user data in a manner protected from *modification* errors.

FDP_UIT.1.2

The TSF shall be able to determine on receipt of user data, whether *modification, deletion, insertion* has occurred.

Application note: This requirement only applies to the following user data: UPLOADED DATA

6.1.4. PROTECTION OF THE TSF

[94] **INTER-TSF TSF DATA CONSISTENCY (FPT_TDC)**

FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *the SHA-256 hash of the encrypted uploaded data* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *rule named “Encrypted file integrity check”* when interpreting the TSF data from another trusted IT product.

Note: The rules “Encrypted file integrity check” is detailed in § “7.1.3 SF_3: USER and TSF data protection”

[95] **TESTING OF EXTERNAL ENTITIES (FPT_TEE)**

FPT_TEE.1: Testing of external entities

FPT_TEE.1.1 The TSF shall run a suite of tests *during the installation* to check the fulfillment of *list of properties of the external entities detailed in Table 20*.

FPT_TEE.1.2 If the test fails, the TSF shall *show in red in the Control Panel the status of the external entity test as “state = KO”*.

External entity	List of properties
BBOP Server	Presence of software prerequisites as specified in §1.5.4.1
Storage system	Presence of connectivity, path of storage system
DBMS	Presence of connectivity required DBMS type

Table 20: list of properties of the external entities

6.1.5. SECURITY MANAGEMENT

[96] **FMT_MTD: MANAGEMENT OF TSF DATA**

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1

The TSF shall restrict the ability to *operations specified in Table 21* the *TSF data specified in Table 21* to *authorized identified roles specified in Table 21*

Authorized roles	TSF Data	Operation Allowed
SAM	TOE company configuration through dashboard	Create, modify, delete
SAM, ADM, ADR with permissions to access the ADMINISTRATION ROLES section on the Dashboard	ADR profile	Create, modify, delete
SAM, ADM, ADR with permissions to access the USERS SETTINGS section on the Dashboard	USR profile	Create, modify, delete
SAM, ADM, ADR with permissions to access the USERS section on the Dashboard	TOE users	Create, modify (user properties), activate, suspend, delete
	TOE users' credential	Create_default, modify, delete
SAM, ADM, ADR with permissions to access the ADMINISTRATION LOGS section on the Dashboard	Audit logs for all activity performed by BooleBox administrative profiles	Query, export
SAM, ADM, ADR with permissions to access the AUDITING section on the Dashboard	Audit logs for all activity carried out by users within the BooleBox platform	Query, export
SAM, ADM, ADR with permissions to access the SHARING TEMPLATES section on the Dashboard	Sharing templates	create, modify, delete, change_default
Authorized USR (user settings.custom sharing=enabled)	Sharing templates	set
SAM, ADM, ADR, USR	Own activity logs	Query
	Permissions on uploaded files	Create_default (classification project), Set, modify, delete
SAM, ADM, ADR, USR, GUEST	password	Change_default.

Table 21: Management of TSF data

Application note: the access control to the Control Panel is delegated to the Operational Environment of the TOE (Operating System) that allows only TOE authorized administrators to execute the Control Panel.

[97] **FMT_MOF: MANAGEMENT OF FUNCTIONS IN TSF**

FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1

The TSF shall restrict the ability, **through the dashboard**, to *determine the behavior of, disable, enable, modify the behavior of* the functions *as specified in Table 22 to roles as identified in Table 22.*

Authorized roles	Ability to	Functions
SAM, ADM, authorized ADR through the dashboard	Enable/disable	Dashboard functionalities for ADRs
	modify the behavior of	User audit function (by changing user log period)
	modify the behavior of	TOE access mode for USR
	Enable/disable	TOE users account
	modify the behavior of	TOE functionalities for ADRs and USRs (changing Users settings)
USR, GUEST	none	none

Table 22: Management of security functions

Application note: the access control to the Control Panel is delegated to the Operational Environment of the TOE (Operating System) that allows only TOE authorized administrators to execute the Control Panel.

[98] **FMT_MSA: MANAGEMENT OF SECURITY ATTRIBUTES**

FMT_MSA.1 (1) Management of security attributes

FMT_MSA.1.1

The TSF shall enforce the *BBOP Administrators access control SFP* to restrict the ability to *change default, query, modify, delete, create* the security attributes *defined in Table 23 to the authorized identified roles specified in Table 23.*

Authorized role	Ability to	Security Attribute
SAM, ADM	Query, change_default	BBOP installation Parameters
SAM, ADM Authorized ADR	create change_default, modify, delete	Username, Password, User Privileges
	query	Current Access attempts.
	create	Personal key
	Change_default	User Type, User status, User Role

Table 23: Management of security attributes

Application note: the access control to the Control Panel is delegated to the Operational Environment of the TOE (Operating System) that allows only TOE authorized administrators to execute the Control Panel.

FMT_MSA.1 (2) Management of security attributes

FMT_MSA.1.1

The TSF shall enforce the *BBOP Users access control SFP* to restrict the ability to *change_default* the security attributes *defined in Table 24* to *the authorized identified roles specified in Table 24*.

Authorized role	Ability to	Security Attribute
Authorized USR	change_default	classification project's membership
SAM, ADM, ADR, USR	change_default	Password, personal key
GUEST	change_default	password

Table 24: Management of security attributes

FMT_MSA.1 (3) Management of security attributes

FMT_MSA.1.1

The TSF shall enforce the *uploaded file access control SFP* to restrict the ability to *change_default* the security attributes *defined in Table 25* to *the authorized identified roles specified in Table 25*.

Authorized role	Ability to	Security Attribute
Authorized USR	change_default	file ownership file sharing template
SAM, ADM, ADR	change_default	file ownership
GUEST	none	none

Table 25: Management of security attributes

FMT_MSA.3 (1) Static attribute initialization

FMT_MSA.3.1

The TSF shall enforce the *BooleBox Administrator access control SFP* to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow the *SAM, ADM, authorized ADR* to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3 (2) Static attribute initialization

FMT_MSA.3.1

The TSF shall enforce the *BBOP Users access control SFP* to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow *the authorized USR* to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3 (3) Static attribute initialization**FMT_MSA.3.1**

The TSF shall enforce the *uploaded file access control SFP* to provide *permissive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2

The TSF shall allow *the authorized USR* to specify alternative initial values to override the default values when an object or information is created.

[99] FMT_SMF SPECIFICATION OF MANAGEMENT FUNCTIONS**FMT_SMF.1 (1) Specification of Management Functions****FMT_SMF.1.1 – Management via dashboard**

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

- *ADMINISTRATION ROLES management*
- *ADMINISTRATION LOGS management*
- *USER management*
- *USER SETTING management*
- *AUDITING management*
- *SHARING TEMPLATE management*
- *CLASSIFICATION projects management*

FMT_SMF.1 (2) Specification of Management Functions**FMT_SMF.1.1 - Management via Control Panel**

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

- *TOE INSTALLATION PARAMETERS management*
- *query TOE status*
- *DBMS/STORAGE INSTALLATION PARAMETERS management*
- *query DBMS/STORAGE status*
- *view results of a DIAGNOSTIC CHECK*
- *update the certificate of the MASTER KEY*

[100] FMT_SMR: SECURITY MANAGEMENT ROLES**FMT_SMR.1 Security roles****FMT_SMR.1.1**

The TSF shall maintain the roles *SAM, ADM, ADR, USR, GUEST*.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.1.6. PRIVACY

[101] FPR_UNO: UNOBSERVABILITY

FPR_UNO.1 Unobservability

FPR_UNO.1.1

The TSF shall ensure that *unauthorized user* are unable to observe the operation *full displaying of the user data* on *end user screen* by *BBOP users*.

Application Note: the requirement is implemented only when the data owner uses a sharing template that includes the Deter Photo Shots option. "Unauthorized user" means all subjects who are not the recipients of the user data.

[102] FPR_PSE: PSEUDONYMITY

FPR_PSE.1 Pseudonymity

FPR_PSE.1.1

The TSF shall ensure that *unauthorized user* are unable to determine the real user name bound to *TOE users data upload*.

FPR_PSE.1.2

The TSF shall be able to provide *one* aliases of the real user name to *TOE users*.

FPR_PSE.1.3

The TSF shall *determine an alias for a user* and verify that it conforms to the *following metric*:
16 byte (128 bit) represented by 32 hexadecimal characters, displayed in five groups separated by dashes, in the format 8-4-4-4-12 for a total of 36 characters

Application Note:

- 1) "Unauthorized user" means all subjects who are not the authorized administrators. An example of alias: 550e8400-e29b-41d4-a716-446655440000
- 2) The aliases are not the "Alias Profiles" indicated in the TOE graphical interfaces but are generated internally by the TOE and are enabled by the administrator by selecting the "Enable Anonymized Alias" option.

6.2. SECURITY ASSURANCE REQUIREMENTS

- [103] The assurance security requirements for this Security Target are taken from Part 3 of the CC according to [CCP3] Table 3. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) augmented by ALC_FLR.2.
- [104] EAL2+ (ALC_FLR.2) is chosen because the TOE is supposed to be used in an operational environment in which the attack potential of an attacker is *basic*.
- [105] The following table describes the security assurance requirements:

CLASS HEADING	CLASS FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documentation	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
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
	ALC_FLR.2	Flaw reporting procedures
ASE: Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended component definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table 26: Security Assurance Requirements

6.3. SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

6.3.1. CC Component Dependencies

[106] This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies.

[107] The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	DEPENDENCY	RATIONALE
FAU_GEN.1	FPT_STM.1	Satisfied by the operational environment (OE.TIME)
FAU_GEN.2	FAU_GEN.1	Satisfied
	FIA_UID.1	Satisfied by FIA_UID.2, hierarchical to FIA_UID.1
FAU_SAR.1 (1)	FAU_GEN.1	Satisfied
FAU_SAR.1 (2)	FAU_GEN.1	Satisfied
FAU_SAR.2	FAU_SAR.1	Satisfied
FAU_SAR.3	FAU_SAR.1	Satisfied
FIA_AFL.1	FIA_UAU.1	Satisfied by FIA_UAU.2, hierarchical to FIA_UAU.1 Satisfied by operational environment (OE.SO) for Control Panel component
FIA_UID.2	-	-
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2, hierarchical to FIA_UID.1 Satisfied by operational environment (OE.SO) for Control Panel component
FIA_UAU.5	-	-
FIA_ATD.1	-	-
FIA_SOS.1	-	-
FDP_ACC.1 (1)	FDP_ACF.1 (1)	Satisfied
FDP_ACC.1 (2)	FDP_ACF.1 (2)	Satisfied
FDP_ACC.1 (3)	FDP_ACF.1 (3)	Satisfied
FDP_ACF.1 (1)	FDP_ACC.1 (1)	Satisfied
	FMT_MSA.3 (1)	Satisfied
FDP_ACF.1 (2)	FDP_ACC.1 (2)	Satisfied
	FMT_MSA.3 (2)	Satisfied
FDP_ACF.1 (3)	FDP_ACC.1 (3)	Satisfied
	FMT_MSA.3 (3)	Satisfied
FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_IFC.1
	FMT_MSA.3	Not Applicable. This FMT_MSA.3 requirement has not been iterated for BooleBox flow control SFP since it is not applicable because the security attributes specified into BooleBox flow control SFP are not manageable by any user role.
FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1	Not Applicable.

	FTP_ITC.1 or FTP_TRP.1	This requirements are not relevant to countering threats and for fulfill the objectives of security because the user data exchanged between BBOP and Storage are transmitted encrypted.
	FPT_TDC.1	Satisfied
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_IFC.1
FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_IFC.1
FDP_IFC.1	FDP_IFF.1	Satisfied

SFR	DEPENDENCY	RATIONALE
FDP_IFF.1	FDP_IFC.1	Satisfied
	FMT_MSA.3	Not Applicable. This FMT_MSA.3 requirement has not been iterated for BooleBox flow control SFP since it is not applicable because the security attributes specified into BooleBox flow control SFP are not manageable by any user role.
FDP_UCT.1	FTP_ITC.1 or FTP_TRP.1	FTP_TRP.1 satisfied by TOE operational environment which implements the https channel to the end user (see [OE.CRYPTO]).
	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_IFC.1
FDP_UIT.1	FTP_ITC.1 or FTP_TRP.1	FTP_TRP.1 satisfied by TOE operational environment which implements the https channel to the end user (see [OE.CRYPTO]).
	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_IFC.1
FPT_TDC.1	-	-
FPT_TEE.1	-	-
FMT_MTD.1	FMT_SMR.1	Satisfied
	FMT_SMF.1 (1)	Satisfied
FMT_MOF.1	FMT_SMR.1	Satisfied
	FMT_SMF.1 (1)	Satisfied
FMT_MSA.1 (1)	FMT_SMF.1 (1)	Satisfied
	FMT_SMR.1	Satisfied
	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.1 (1)
FMT_MSA.1 (2)	FMT_SMF.1 (1)	Satisfied
	FMT_SMR.1	Satisfied
	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.1 (2)
FMT_MSA.1 (3)	FMT_SMF.1 (1)	Satisfied
	FMT_SMR.1	Satisfied
	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.1 (3)

FMT_MSA.3 (1)	FMT_MSA.1 (1)	Satisfied
	FMT_SMR.1	Satisfied
FMT_MSA.3 (2)	FMT_MSA.1 (2)	Satisfied
	FMT_SMR.1	Satisfied
FMT_MSA.3 (3)	FMT_MSA.1 (3)	Satisfied
	FMT_SMR.1	Satisfied
FMT_SMF.1 (1)	-	-
FMT_SMF.1 (2)	-	-
FMT_SMR.1	FIA_UID.1	Satisfied by FIA_UID.2, hierarchical to FIA_UID.1
FPR_UNO.1	-	-
FPR_PSE.1	-	-

Table 27: TOE SFR dependency rationale

6.3.2. Tracing between SFRs and the security objectives for the TOE

SFR/O	O.AUDIT	O.AUDIT_PROT	O.USER	O.IDENTIFY	O.ANTI_BRUTE	O.ACCESS	O.MANAGE	O.CONFIDENTIAL	O.CRYPTO	O.INTEGRITY	O.CONFIG	O.OTP	O.STRONG_PERSONALKEY	O.PRIVACY
FAU_GEN.1	X													
FAU_GEN.2	X													
FAU_SAR.1	X													
FAU_SAR.2	X													
FAU_SAR.3	X													
FIA_AFL.1					X									
FIA_UID.2				X		X								
FIA_UAU.2				X		X								
FIA_UAU.5						X						X		
FIA_ATD.1						X								
FIA_SOS.1				X									X	
FDP_ACC.1						X	X		X					
FDP_ACF.1						X	X		X					
FDP_ITC.1									X					
FDP_ITC.2								X	X					
FDP_ETC.1									X					
FDP_ETC.2								X	X					
FDP_IFC.1		X						X	X					
FDP_IFF.1		X						X	X					
FDP_UCT.1								X						
FDP_UIT.1										X				
FMT_MTD.1			X			X	X							
FMT_MOF.1			X				X							
FMT_MSA.1			X			X								
FMT_MSA.3			X			X								
FMT_SMF.1							X							
FMT_SMR.1						X	X							
FPT_TDC.1										X				
FPT_TEE.1											X			
FPR_UNO.1								X						
FPR_PSE.1														X

Table 28: Mapping of TOE SFRs to Security Objectives

[108] The following table provides detailed evidence of coverage for each security objective.

OBJECTIVE	RATIONALE
O.AUDIT	<p>Security-relevant events must be defined and auditable for the TOE and the user associated with the events must be recorded [FAU_GEN.1, FAU_GEN.2].</p> <p>The TOE provides SAM, ADM, ADR, USR users with the capability to read a specific set of audit information and the ability to apply searches of audit based on date of the event, type of event and subject identity. [FAU_SAR.1, FAU_SAR.2, FAU_SAR.3].</p>
O.AUDIT_PROT	<p>The TOE enforces the integrity and confidentiality protection of audit information generated by itself, because they are store encrypted on the DBMS according to BooleBox flow control SFP [FDP_IFC.1, FDP_IFF.1].</p>
O.USER	<p>Only authorized administrators (SAM, ADM, authorized ADR) are allowed to create/delete, activate/suspend TOE users [FMT_MTD.1, FMT_MOF.1], and configure them and modify user properties limiting their access to TOE functionalities. [FMT_MSA.1, FMT_MSA.3].</p>
O.IDENTIFY	<p>Users authorized to access the TOE are determined using an identification process upon username/password combination [FIA_UID.2 and FIA_UAU.2].</p> <p>The TOE specifies metrics for password complexity in authentication [FIA_SOS.1]. See also O.OTP rationale.</p>
O.ANTI_BRUTE	<p>The TOE requires that the TSF shall be able to terminate the session establishment process after three unsuccessful user authentication attempts.</p> <p>It also requires that, when three unsuccessful authentication attempts has been met, <i>the user insert a captcha code foreseeing an increasing delay for each wrong captcha code inserted.</i> [FIA_AFL.1].</p>
O.ACCESS	<p>Security attributes of subjects used to enforce the security policy of the TOE must be defined [FIA_ATD.1].</p> <p>Users authorized to access the TOE are determined using an identification and authentication process based not only on a couple {username, password} but also on providing a valid OTP [FIA_UAU.2, FIA_UID.2, FIA_UAU.5] [FDP_ACC.1] [FDP_ACF.1].</p> <p>The TOE maintains the following roles [FMT_SMR.1]: SAM, ADM, ADR, USR, GUEST.</p> <p>The permitted access to TOE data by the roles and permissions is defined [FMT_MTD.1]. The management of security attributes is restricted to authorized roles [FMT_MSA.1.].</p> <p>The default values of security attributes are permissive in nature [FMT_MSA.3].</p>

OBJECTIVE	RATIONALE
O.MANAGE	<p>Specification of Management functions requires that the TSF provide specific management functions [FMT_SMF.1].</p> <p>Management of TSF data allows authorized users to manage TSF data [FMT_MTD.1].</p> <p>Management of security functions behavior allows the authorized users (roles) to manage the behavior of functions in the TSF that use rules or have specified conditions that may be manageable [FMT_MOF.1], according to BBOP Administrators access control SFP [FDP_ACC.1, FDP_ACF.1].</p> <p>Security roles specifies the roles with respect to security that the TSF recognizes [FMT_SMR.1].</p>
O.CONFIDENTIAL	<p>According to BooleBox flow control policy [FDP_IFC.1], [FDP_IFF.1] uploaded data are stored encrypted on the storage, after having stored on the DBMS a related record of security attributes [FDP_ETC.2]; they can be retrieved by the file owner if the integrity check succeeds [FDP_ITC.2].</p> <p>User data transfer are protected from unauthorized disclosure [FDP_UCT.1].</p> <p>With “Deater Photoshots” option activated the TOE ensure that unauthorized user are unable to observe the entire screen of the user while consult his file. [FPR_UNO.1].</p>
O.CRYPTO	<p>[FDP_IFC.1] and [FDP_IFF.1] establish BooleBox flow control security policy which lay down the rules that the TOE must follow to ensure that the exchange of user data between the TOE and Storage takes place only if the user data are encrypted.</p> <p>[FDP_ITC.2] and [FDP_ETC.2] enforce the BooleBox flow control security policy ensuring that security attributes correctly represent the user data and are accurately and unambiguously associated with the user data imported and exported from Storage system, by the data owner [FDP_ACC.1, FDP_ACF.1].</p> <p>[FDP_ITC.1] and [FDP_ETC.1] enforce the BooleBox flow control security policy granting that other user data are transferred to and from the TOE after being encrypted.</p>
O.INTEGRITY	<p>The TOE implements Encrypted file check rule when interpreting the TSF data from DBMS during data upload [FPT_TDC.1].</p> <p>The TOE implements a control access security policy and a flow control security policy to prevent modification of user data when transmitted outside the TOE (to/from DB and to/from storage) [FDP_UIT.1].</p>
O.CONFIG	<p>The TOE, during installation process, performs tests on external entities in order to ensure compliance with the pre-required software. [FPT_TEE.1].</p>
O.OTP	<p>The TOE implements a multiple authentication mechanism based on static password (PASSWORD) and One Time Password that is sent to the user via cell phone number [FIA_UAU.5].</p>
O.STRONG_PERSONALKEY	<p>When a TOE user defines a personal key to access a specific file the TOE requires that it satisfies the same complexity criteria as defined for users’ passwords [FIA_SOS.1].</p>
O.PRIVACY	<p>The TOE grants TOE users Pseudonymity during data upload [FPR_PSE.1].</p>

Table 29: Rationale for TOE Security Objectives coverage by SFRs

7 TOE SUMMARY SPECIFICATION

7.1. SECURITY FUNCTION

[109] The security functions described in the following subsections fulfill the security requirements that are defined in Section 6.1 – Security Functional Requirements. The security functions performed by the TOE are as follows:

SF_1 = Identification and Authentication
 SF_2 = Security Audit
 SF_3 = USER data and TSF data protection
 SF_4 = Security Management
 SF_5 = Access control
 SF_6 = Privacy

[110] The following paragraphs describe the security features implemented by the TOE and how they are implemented.

7.1.1. SF_1: Identification and Authentication

[111] The TOE users must login with a valid Username and Password and a valid OTP. The Guest user can access a shared file only after setting a static password without the need of OTP password.

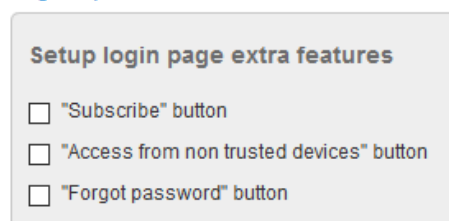
[112] If the authentication attempt is successful, the TOE grants access to TOE functionalities. If the validation is not successful than:

[113] In case of an incorrect login by a user the login procedure is repeated, but after three failed login attempts, the user is asked to enter a captcha code in addition.

[114] In case of incorrect captcha code insertion the TOE ask again the user to insert e captcha code foreseeing an increasing delay for each wrong captcha code inserted.

[115] The following login options are available to TOE users, according to what has been defined by an authorized administrator:

Login Options



Setup login page extra features

"Subscribe" button

"Access from non trusted devices" button

"Forgot password" button

“subscribe” button:

When checked it means that the users will be asked (una tantum) to register, providing their personal data, before accessing BBOP services.

“access from non-trusted devices” button

When checked it means that the users, that must have provided their email, will be allowed to access BBOP from unsecure devices: in case of login from untrusted device, users will then receive on their mobile a one-time-password valid for one single access. In the certified version of the product the "access from non trusted device" login option is not shown to the TOE user as the OTP is in any case sent to the user except for the Guest user.

“forgot password” button

When checked it means that the users will be provided, in the login mask, with a button to request the forgotten password. By clicking on "forgotten password" the user must enter the e-mail address linked to his account and wait for the password recovery e-mail. The user can then create a new password and log in to his / her private area.

7.1.2. SF_2: Security Audit

- [116] Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities, i.e. each action performed by TOE users on TOE data and functions. The resulting audit records can be examined by the authorized administrator to determine which security-relevant activities took place and who (i.e., which user) is responsible for those activities.
- [117] The Security audit function is always active after BBOP installation and set up to operation and cannot be stopped. Other non-security related events are logged together with those listed in Table 30 and Table 31.
- [118] Each action logged includes the date and time of the event, the ID of the user that caused the action, the IP address of End User’s device and the type (name) of the event. The outcome (success or failure) of the events is not recorded: all events are registered when have success outcome. The Login with failure outcome is recorded as a “Login Failed” event.
- [119] Audit logs are stored encrypted on the DBMS according to the BooleBox flow control SFP.
- [120] **Auditing of SAM/ADM log:** Through the dashboard provided by BBOP Server, the SAM/ADM/authorized ADR can view the log of the operations performed by administrative users. The categories of administrative auditable operations relevant for security are listed in Table 30. It is also possible filter the events by defining a time range which by default is set to 1 day.

Administrative (SAM/ADM/authorized ADR) Profile– Security relevant Auditable events categories	
USERS	New user
	Edit user
	Delete user
	Change status
	Change settings
	External user invitation/addition
USERS SETTINGS	Add settings
	Edit settings
	Apply settings (to one or more user)
	Delete settings (the template is deleted)
SHARING TEMPLATES	Add share template
	Edit share template
	Delete share template
	Add members to share template
	Remove members from share template
ADMINISTRATION ROLES	Add role
	Edit role
	Delete role
	Add members to role
	Remove members from Role
CLASSIFICATION	Add project
	Edit project
	Change status (show/archive)
	Add administrator
	Remove administrator
	Delete project
	Add Tags to project
	Edit project’s tag
	Add members to tag
	Remove members from tags
	Edit tags protection
	YOUR ACCOUNT

Table 30: Category of Security Relevant Auditable Events for Administrative profile

[121] **Auditing of USR log:** Through the dashboard provided by BBOP Server, the SAM/ADM/authorized ADR can view the log of the operations performed by users with role USR. Beside each USR user can view the log of the operations performed, on files he owns, both by himself and by other users to whom those files have been shared. The categories of USR auditable operations relevant for security are listed in Table 31. It is also possible filter the events by defining a time range which by default is set to 1 day.

USR Profile – Security relevant Auditable events categories	
ACCESS	Login
	Login Failed
	Logout
	Change Account
	Switch Account
FILE	New folder
	Cut & paste
	Copy & paste
	Rename
	Delete file
	Show file
	Edit file
	New file
	Download file
	Upload file
	Search file
	Versioning view
	Empty bin
	Delete file from recycle bin
	Restore file from recycle bin
	Share
	Cut & paste sharing properties
	Copy & paste sharing properties
	Delete share
	Tag
	Delete tag
	Print file
	Apply personal key
	Remove personal key
	Add to bookmarks
	Classification
	Remove classification
Previous versions	
Change ownership	
YOUR ACCOUNT	Change password

Table 31: Category of Security relevant Auditable Events for USR profile

[122] The BooleBox accounting services allow the SAM/ADM profile to set users log period (Log file of all operations performed by any BooleBox end users is stored encrypted in the database for a configurable period set by default equal to 365 days);

[123] All events, recorded and stored encrypted within the DB through audit functions, could then be filtered by categories.

7.1.3. SF_3: USER data and TSF data protection

- [124] With reference to § 1.6.5, The TOE protects the following USER DATA:
- Personal information related to user account, created in BBOP and sent to the DB AES-256 encrypted with the MASTER KEY with the support of the operational environment;
 - Uploaded data received by the server where BBOP is installed: BBOP ask the environment to AES-256 encrypt them with the MASTER KEY (the default for each file) or with a PERSONAL KEY defined by the data owner and save them on the storage;
 - Email messages, when requested: instead of files, BBOP ask the environment to AES-256 encrypt email messages which are saved only on the DBMS and not also on the storage.
- [125] With reference to § 1.6.5, The TOE protects each TSF DATA:
- TOE MASTER KEY (256 bit long) generated at installation time and different for each BBOP instance and stored AES-256 encrypted with the support of the operational environment in the disk of the server where BBOP is installed with the K_{pub} on the certificate uploaded during BBOP setup;
 - TOE configurations {dashboard parameter settings as company configurations, users setting, etc.}, stored AES-256 encrypted in the DBMS;
 - TOE Users' credentials: ID (stored AES-256 encrypted on DBMS) and SHA-256 hash of the PASSWORD stored on DBMS;
 - AUDIT LOGS: generated on BBOP and stored in the DBMS after being AES-256 encrypted using the MASTER KEY;
 - Sharing templates: sets of rules defined in BBOP, managed by the administrators and stored in DBMS tables AES-256 encrypted using the MASTER KEY.
- [126] BooleBox uses a different randomly generated MASTER KEY for each installation (see next figure below). The random generation functionality (RNG) is provided by the operational environment (Microsoft .Net GUIDE + CNG - Cryptography API: Next Generation) Features).

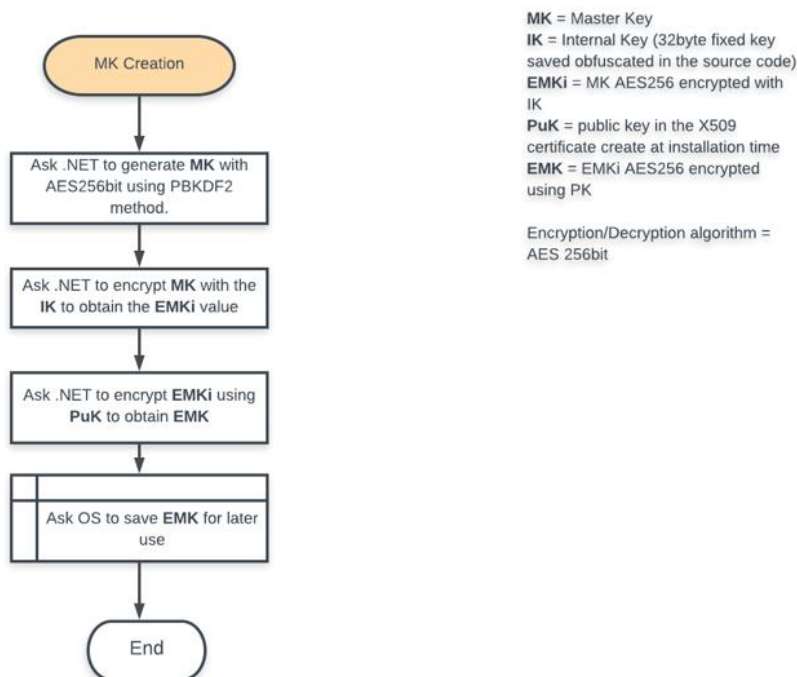


Figure 7: MASTER KEY creation process

- [127] With the support of the operational environment, i.e. by underlying operating system, USER DATA listed above when received by BooleBox are AES-256 encrypted with the MASTER KEY and stored in the storage system or in the DB according to BooleBox flow control security policy. When requested, USER DATA are decrypted and, if the integrity check succeeds, they are retrieved (see next figure).
- [128] Uploaded data could be AES-256 encrypted with a PERSONAL KEY defined by the data owner instead of the MASTER KEY. In this case BBOP asks the operating system to decrypt the file previously encrypted with the MASTER KEY and to encrypt it again with the PERSONAL KEY.
- [129] To ensure the confidentiality of information protected by BooleBox, the MASTER KEY is stored encrypted in the DB and any PERSONAL KEY is never stored by BBOP.
- [130] **Encrypted file integrity check**

When an encrypted owned file needs to be read from the Storage, the SHA-256 hash of encrypted file is calculated and then compared with the same hash previously calculated and stored in the DB. The hash is used to detect any random changes that occurred during the permanence of the file on the storage system. If this comparison fails BBOP retrieve an error message and it denies the data retrieval; otherwise the required user data are transferred from Storage to BB Server.

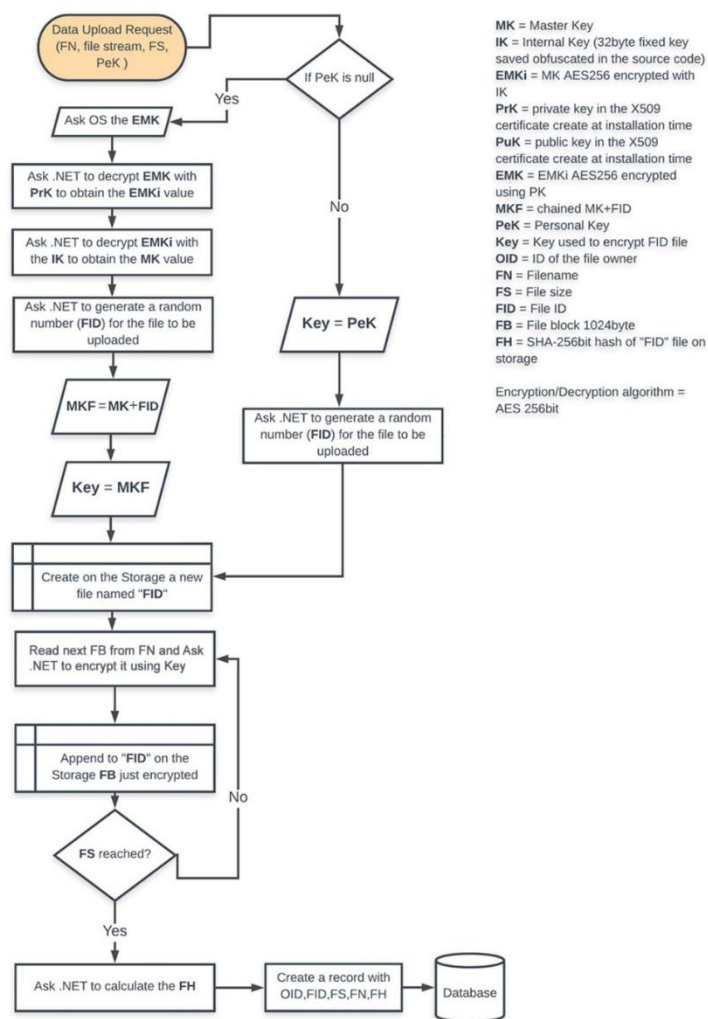


Figure 8: file encryption process

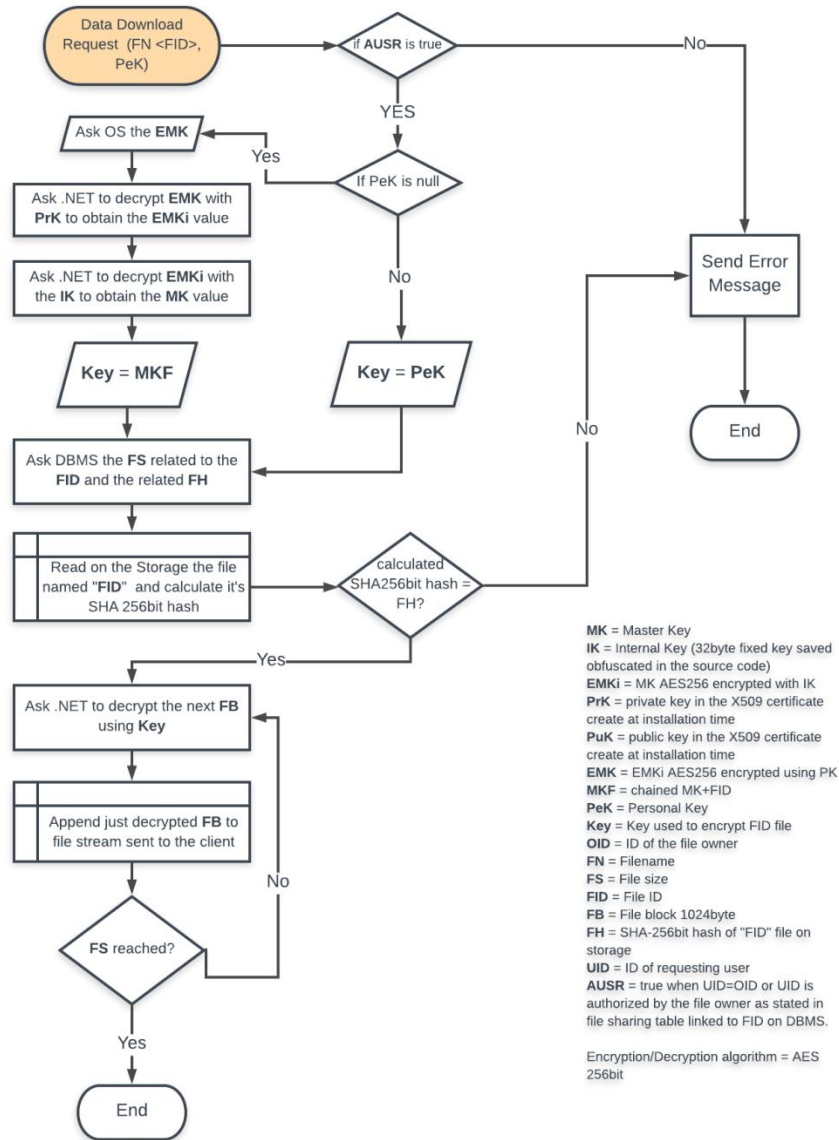


Figure 9: file decryption process

- [131] Furthermore, note that BBOP operational environment is configured to establish always an HTTPS channel based on AES 256 between End user and Server.
- [132] The operational environment supports the TOE functions by implementing random number generation and RSA 2048-bit encryption during the initial handshake upon setting up the secure channel

7.1.4. SF_4: Security Management

- [133] BooleBox 's allows real time editing of any users rights at any time; as well, access to information can be instantly revoked even after information has been shared.
File security is granted at all stages - "in motion" as well as "at rest". The TOE's management security function provides administrator support functionality to configure and manage TOE.
- [134] Management of the TOE is performed via Dashboard and Control Panel.
- [135] **MANAGEMENT OF THE TOE VIA DASHBOARD**
Below are described the functions that the BBOP allows an authorized administrator (SAM, ADM or ADR properly configured) to manage through its dashboard.

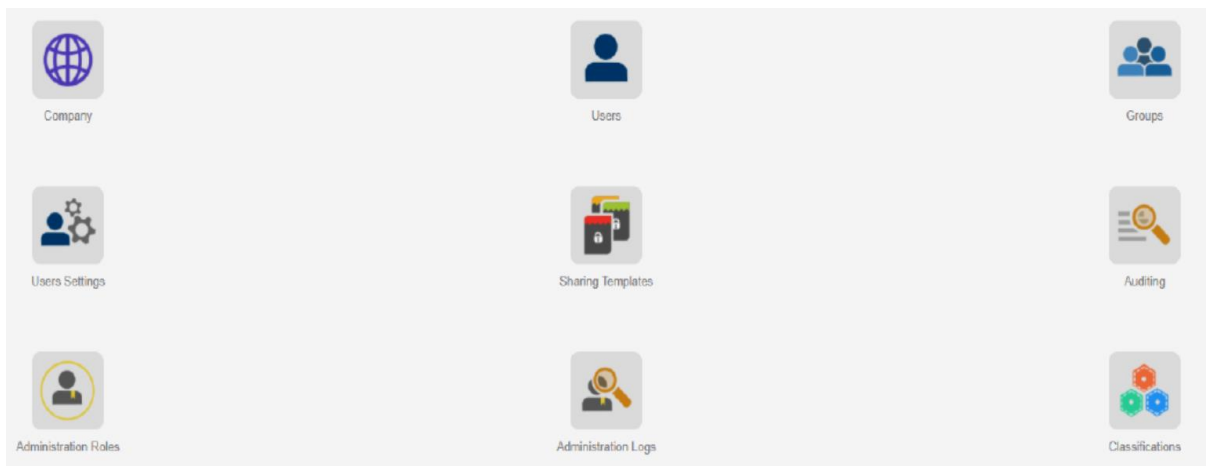


Figure 10: The Dashboard

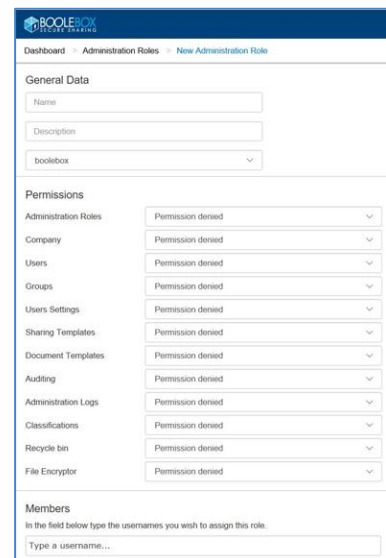
- **Administration roles→**

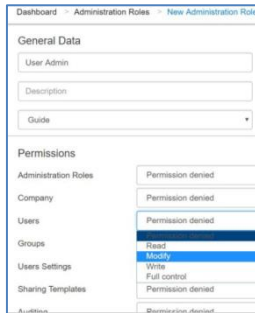
to create and manage ADMINISTRATIVE "RESTRICTED" ROLE (ADR) profiles which can be assigned to Administrators who are authorized to access the DASHBOARD section (see figures on the right).

In the GENERAL DATA section it must be entered the NAME ("User Admin" in the example) to be assigned to the new Administrative restricted role (ADR) in the appropriate field and a brief DESCRIPTION in the relevant field summarizing the role being configured.

In the MEMBERS area, it must be indicated the username (i.e. the email address) of those to whom the ADMINISTRATIVE "RESTRICTED" ROLE (ADR) will be applied.

Once defined, an ADR can be modified or deleted by those administrators who have the proper "Administrator roles" permission (MODIFY or FULL CONTROL).



**NOTE:**

It is not possible to change the company to which the profile has been assigned during the creation phase.

User privileges can be set equal to:

- PERMISSION DENIED (i.e. no permission)
- READ ONLY permission
- MODIFY permission for existing setting
- WRITE permission for new settings
- FULL CONTROL (i.e. it is also possible in BBOP to create a new ADR administration profile, different from ADMIN (ADM), with all privileges set to FULL CONTROL)

- **Users** →

create, remove, set password, manage (Show details/Delete/Set Password/Suspend/activate/edit settings) the USR profiles for a specific COMPANY.

Add to COMPANY an external GUEST user, so becoming an internal TOE USR user.

- **User settings** →

Definition new USR profiles that can be assigned to groups of users that are part of a COMPANY. Users can be assigned to groups of users that are part of a COMPANY, but please note that groups of user can be manage but there aren't any access control policies based on belonging to a group or not. The DEFAULT profile defines the features that will be applied to all new users that will be added to the current company. The DEFAULT PROFILE SETTINGS can be edited and new user profile can be defined, in particular specifying settings for:

- **Access Notification** → If enabled, this option sends an email from BooleBox to the user each time their account is used to log in. By default, this option is disabled but can be changed by the user. To ensure that users do not independently change the assigned value, it is sufficient to deactivate the associated command in the EDITABILITY column.
- **Single Sign On** → If enabled, this option allows users to access BooleBox without having to enter their username and password each time, following their first login. By default, this option is disabled but can be changed by the user. To ensure that users do not independently change the assigned value, it is sufficient to deactivate the associated command in the EDITABILITY column. In the certified version of the product the Single Sign On feature must not be activated. This functionality must not be activated by non-administrative users.
- **Personal Key** → If enabled, this option allows users to use the Personal Key encryption feature. By default, the option is activated.
- **Custom sharing** → If enabled, this option allows users to customize the sharing properties, by having not only predefined

sharing templates available, but also sharing options that can be customized in real time. By default, the option is activated.

- **External sharing**→ If enabled, the option allows users to share with companies other than that of which they are a member.
 - **Public sharing**→ If enabled, this option allows PUBLIC sharing by users, i.e. files can also be sent to unprofiled users as they will not be asked to authenticate during login. By default, the option is unactivated.
 - **Sharing mode**→ It is possible to activate the options associated with the different modes that may be available to users to enable sharing within the platform. In fact, BooleBox allows sharing via EMAIL, LINK or FACEBOOK. All options are enabled by default.
 - **Section Visibility**→ Options associated to the sections (FILE MANAGER, SECURE MAIL, ACTIVITY LOGS) available to users can be enabled by accessing their BooleBox account. All options are enabled by default.
- **Sharing templates** → create, modify and customize predefined templates for sharing properties based on specific security needs.
 - **Auditing**→ query the log for all activity carried out by users (*Note: In any case an administrator is not allowed to access user data, except for user data belonging to a classification project*) and set Users log period, i.e. the period in which all operations performed by any BooleBox end users are logged and stored encrypted in the database.
 - **Administrative Logs**→ query the log for all activity performed by BooleBox administrative profiles.
 - **Classifications**→ create, modify and customize classification projects to simplify the process of applying centralized security policies through which different functional permissions can be applied to certain types of classifications according to each user.

The following figure shows the interface used by an authorized administrator to create a classification project, named “Demo”. Note that the *administration* of the classification project can be delegated to other TOE users.

The *delegated* classification project administrator are only allowed to decide to which TOE users the file with a specific classification will be accessible.

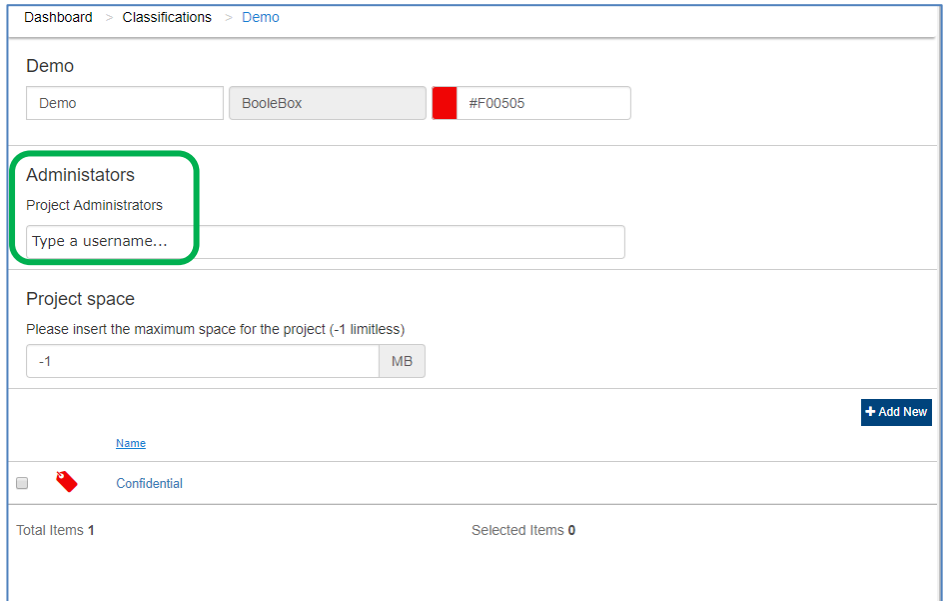


Figure 11: Classification Project creation

The following figure shows instead the interface:

- used by an authorized administrator to define which TOE users can assign a specific classification to a file (green box).
- used by an authorized administrator or a delegated administrator to decide which are the members of a classification project, i.e. to whom (not only the file owner) and how the file or email belonging to a classification project will be accessible (light blue box).

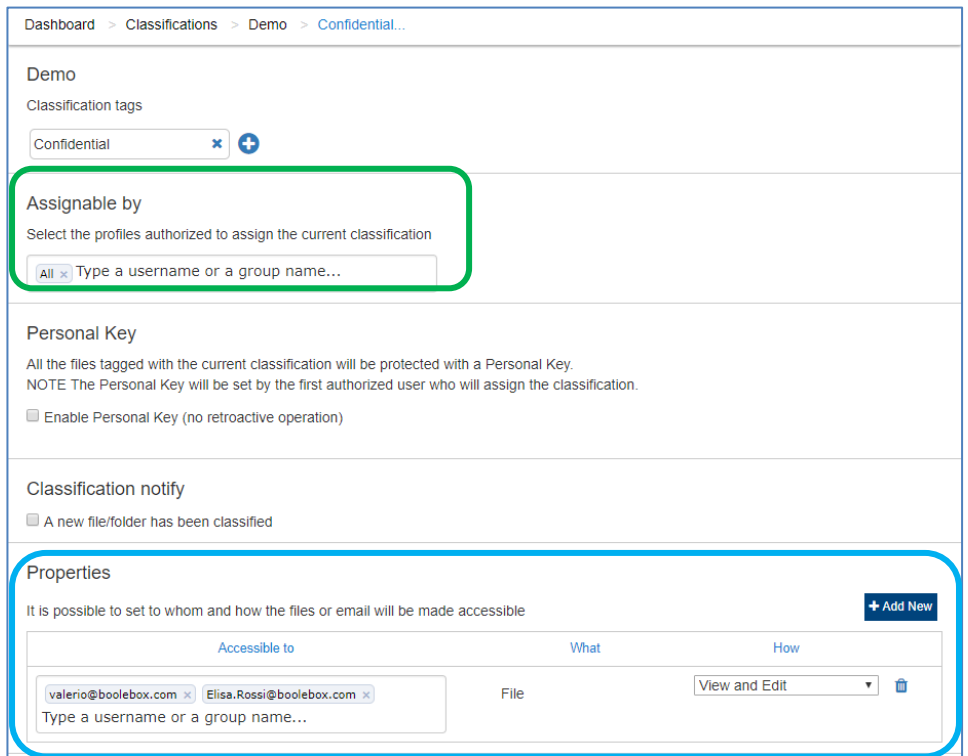


Figure 12: Classification Project configuration

[136] **MANAGEMENT OF THE TOE VIA CONTROL PANEL**

The settings for all BooleBox On-Premises components are accessible from the control panel, available using the relevant desktop shortcut after the installation of the server application is completed.

The self-diagnosis process activates when BooleBox On-Premises is launched, and its results are shown in the Status panel within a few seconds. The control panel is used to obtain information relating to the license to check for updates. The BooleBox On-Premises application logs will also be able to be queried from the control panel.

The following figure shows the Control Panel.

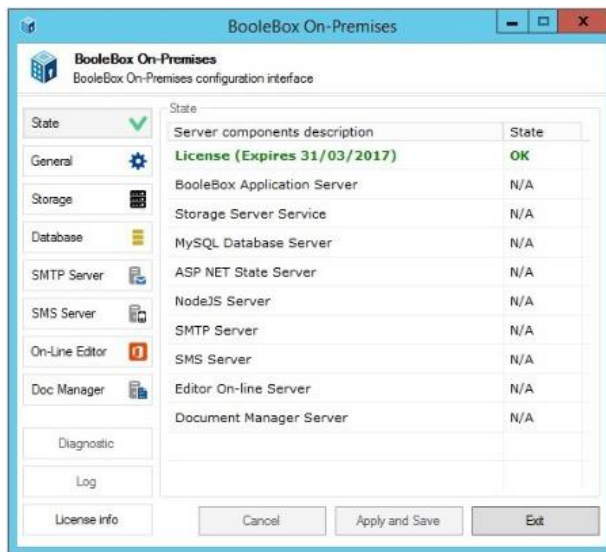


Figure 13: The Control Panel

Below are the functions that the BBOP allows an authorized administrator to manage through its control panel.

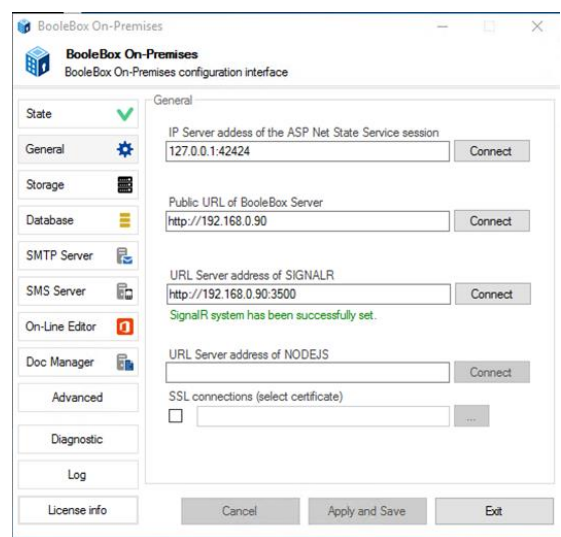
- **TOE INSTALLATION PARAMETERS management**

The GENERAL section of the Control Panel allow the configuration of BBOP parameters as shown in the figure on the right.

- **query TOE/DBMS/STORAGE status**

The main area of the control panel allows the BooleBox On-Premises services to be monitored. The self-diagnosis process activates when BooleBox On-Premises is launched and its results are shown in the Status panel within a few seconds. Each BooleBox service can have one of the following statuses:

- OK (green): The service is active.
- KO (red): The service is not active or incorrectly installed/configured.
- N/A (gray): The service is not installed.
- UPDATE (yellow): The service requires an update.



• **DBMS/STORAGE INSTALLATION PARAMETERS management**

The STORAGE screen displays all the information relating to the BooleBox Storage server and is used to monitor communication with the service.

The BOOLEBOX STORAGE section can be configured only after completing the installation of the BooleBox Storage server:

- SERVER STORAGE SERVICE URL need to be configured with the IP address of the server on which the service is installed.
- STORAGE ACCESS KEY: need to be configured with an alphanumeric password used to protect saved items.

The DATABASE screen displays all the information relating to the Database used by BooleBox On-Premises. To configure this section it is necessary to have MySQL installed and configured, then it is possible to configure the fields listed below:

- DATABASE SERVER ADDRESS field needs to be configured with the IP address of the server on which MySQL is installed.
- DATABASE CATALOG NAME field needs to be configured with the Name of the database automatically created by clicking on DATABASE TEST.
- DATABASE USER and DATABASE PASSWORD fields need to be configured with the: User access credentials for those with full permissions on the new database to be generated.
- POOL SIZE fields need to be configured with the number of connections you wish to set on the application

DATABASE TEST is the button with which it is possible to:

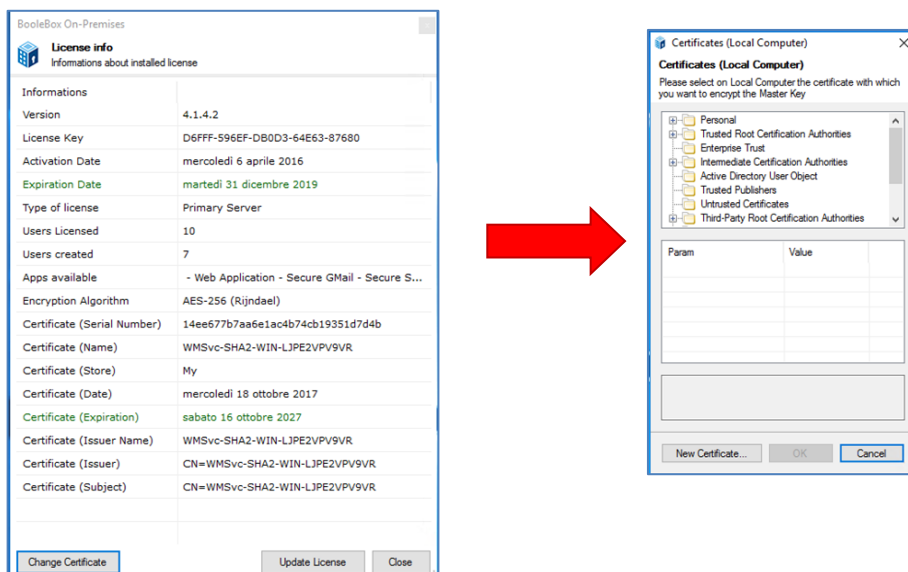
- Generate a new database, if one has not been created previously
- Monitor the status of a connection
- Update a database, for example in the event of an upgrade.

• **view results of a DIAGNOSTIC CHECK**

with the DIAGNOSTIC button it is possible to request a diagnostic check on the status of the TOE / DBMS / STORAGE (and of other elements external to the TOE whose presence / absence has no impact on the TOE security functionalities). At the end of the check it is possible to see the results by clicking on the LOG button of the control panel.

• **UPDATE THE CERTIFICATE OF THE MASTER KEY**

Clicking on the “License Info” button on the Control Panel the following window is opened, from which the certificate of the MASTER KEY can be updated, in case SAM/ADM are aware of its confidentiality violation.



7.1.5. SF_5 Access Control

[137] The access to the Operating System where the TOE is installed is allowed only to TOE authorized administrators, so the Control Panel can be executed and used only by TOE authorized administrators.

The user profiles managed by BooleBox On Premises V. 4.2 that are authorized to access to TOE security functionalities are detailed below.

[138] **SUPER ADMIN (SAM)**

SUPER ADMIN is the predefined role with permissions for creating new companies in addition to the maximum permissions for each company created that are granted to ADMIN (ADM) users. This role is not configurable. The COMPANY section of the dashboard allows SAM to create/delete a COMPANY and to change the setting of a previously created COMPANY. SAM is an administrative profile created automatically during system configuration. The SAM user is set with a default password, which must be changed on first access.

[139] **ADMIN (ADM)**

ADMIN is the predefined and not configurable role with maximum permissions (i.e. FULL CONTROL) within a given company.

A user with the ADM role is authorized to edit all the settings available on the BooleBox application, has full access rights to access and use security relevant TOE functions offered by Dashboard and accessible from the following sections (see SF_4: Security Management for a detailed description of administration functionalities accessible from each Dashboard section):

- **ADMINISTRATION ROLE**
- **USERS**
- **USER SETTINGS (Access Notification, Single Sign On, Personal Key, Custom sharing, External sharing, Public sharing, Sharing mode, Section Visibility)**
- **SHARING TEMPLATES**
- **AUDITING**
- **ADMINISTRATIVE LOGS**
- **CLASSIFICATIONS**

SAM and ADM role can define other administrative “restricted” roles (ADRs) through ADMINISTRATION ROLES section of the Dashboard defining, in the PERMISSIONS area, the specific settings that will define the new ADMINISTRATION ROLE. For each PERMISSION, it is possible to indicate whether the Administrative Restricted Role (ADR) will have: PERMISSION DENIED, READ only, MODIFY permissions for existing settings, WRITE permissions for new settings, or FULL CONTROL.

SAM, ADM and authorized ADR may create and delete another SAM/ADM/ADR but at least one Sam and one ADM must always be defined in BBOP. The major difference between the ADM profile and the ADR profile is that the ADM profile has full access to the dashboard, while other ADR administrators have access only to the dashboard sections selected by a SAM/ADM user during their creation.

SAM, ADM and authorized ADR (i.e. with access to the USER section of the Dashboard) can create/remove (and also set passwords/manage) TOE users with USR profile. Each new user created with USR role by an authorized administrator will be assigned a DEFAULT profile. The DEFAULT profile defines the features that will be applied to all new users that will be added to the current company. In the EDIT PROFILE SETTINGS area an authorized administrator can configure the

specific settings of the DEFAULT profile. By modifying the settings associated with this profile, all subsequently created users will inherit its characteristics.

Through the dashboard an authorized administrator with access to USER section of the Dashboard can redefine a GUEST user (external user) as an internal user with profile USR.

[140] **Administrative restricted role (ADR)**

The ADR is allowed to perform administrative task, according to permissions set by SAM/ADM at its creation that can be a limited set of administrative permissions or also the FULL CONTROL for each administrative permissions as explained in § 7.1.4 SF_4: Security Management.

[141] **User (USR)**

The USR has no access nor to the control panel functions neither to any dashboard functions.

A TOE user with USR role can access to BBOP and, depending on the privilege granted by an authorized administrator with access to the USER SETTINGS section of the Dashboard, he can perform several actions in its workspace and he can dispose of some space for centralized storage of files. See the example schematized in the figure below.

Authorized TOE users (i.e. a file owner having the CUSTOM SHARING permission) can change the sharing permission on a previously shared file at any time. In Table 18 are detailed the sharing permission that can be set by the owner of a file defining a specific sharing template.

Each TOE user is allowed to change his password to access the TOE.

Each TOE user has full access to files he owns.

A TOE user to which a file has been shared receives a notification by email from the file owner that he will be able to access the file, according to its settings and respecting the security levels defined by the file owner: has restricted permissions to access the shared file according to the sharing template associated to it (see Table 18: file sharing permissions configurable in a sharing template). Note that the file owner having the CUSTOM SHARING permission can change the sharing permission on a previously shared file at any time and he is able to notify the recipient of the changes in any moment or to not notify anything at all.

Furthermore, TOE users defined as members of the classification project can open the classified file in the manner set out in the classification project and according to the sharing template specified in the classification project definition. The members of the classification project are TOE users who belong to the group of people to which the file is accessible according to the rules defined by one of the classification project administrators.

According to classification template settings, BooleBox protects file contents even when viewed in clear for example from screenshot, video grabbing, copy and paste. Advanced security features, such as Anti-Capture and Deter Photo Shots reduce risks related to screen capture activities (through Print Screen system functionalities and video grabbing software) while viewing confidential documents. See Table 18: file sharing permissions configurable in a sharing template

[142] **Guest (G)**

Guest profile is assigned to an “external” subject to which data are shared by a BooleBox user with profile SAM, ADM, ADR or USR. Guest profile does not dispose of any space for centralized storage of files and is not allowed to upload files but is enabled to access the shared resources they have received, according to the sharing properties they have been assigned (i.e. through their sharing template). Note that through the dashboard an authorized administrator with access to can redefine a GUEST user as an internal user with profile USR.

Option		Value	Edibility
Access Notification			
Single Sign On			
Two step verification			
Personal Key			Not Available
Custom Sharing			Not Available
Managing your contacts			Not Available
External sharing			Not Available
Public Sharing			Not Available
Empty recycle bin			Not Available
Sharing mode		<input checked="" type="checkbox"/> Mail <input checked="" type="checkbox"/> Link <input checked="" type="checkbox"/> Facebook	Not Available
Section visibility		<input checked="" type="checkbox"/> File Manager <input checked="" type="checkbox"/> Secure Mail <input checked="" type="checkbox"/> Activity Logs	Not Available
Tabs visibility		<input checked="" type="checkbox"/> Files <input checked="" type="checkbox"/> Received <input checked="" type="checkbox"/> Shared <input checked="" type="checkbox"/> Personal Key <input checked="" type="checkbox"/> Favourites <input checked="" type="checkbox"/> Recycle Bin	Not Available
Online Editor		<input checked="" type="checkbox"/> Microsoft Office Online	Not Available
Language		<input type="text" value=""/>	Not Available
Space assigned (GB)		<input type="text" value="100"/>	Not Available
Versions to be saved		<input type="text" value="100"/>	

Figure 14: Example of end-user settings

7.1.6. SF_6 Privacy

[143] BBOP with the support of its operational environment stores TOE users’ personal information (e-mail address, phone number, account credentials) in encrypted format in the DBMS and provides an alias for each user: thus it’s not possible to determine the real user name bound to specific operations performed by users.

7.2. TOE SUMMARY SPECIFICATION RATIONALE

[144] This section demonstrates that the TOE’s Security Functions completely and accurately meet the TOE SFRs. The following table provides a mapping between the TOE’s Security Functions and the SFRs.

	SF_1: Identification and authentication	SF_2: Security Audit	SF_3: USER and TSF data protection	SF_4 Security Management	SF_5: Access control	S SF_6: Privacy
FAU_GEN.1		X				
FAU_GEN.2		X				
FAU_SAR.1		X				
FAU_SAR.2		X				
FAU_SAR.3		X				
FIA_UID.2	X					
FIA_UAU.2	X					
FIA_UAU.5	X					
FIA_AFL.1	X					
FIA_SOS.1	X				X	
FIA_ATD.1	X					
FDP_ACC.1				X	X	
FDP_ACF.1				X	X	
FDP_ITC.1			X			
FDP_ITC.2			X			
FDP_ETC.1			X			
FDP_ETC.2			X			
FDP_IFC.1		X	X			
FDP_IFF.1		X	X			
FDP_UCT.1			X			
FDP_UIT.1			X			
FPT_TDC.1			X			
FPT_TEE.1			X	X		
FMT_MTD.1				X		
FMT_MOF.1				X		
FMT_MSA.1				X		
FMT_MSA.3				X		
FMT_SMF.1				X		
FMT_SMR.1				X	X	
FPR_UNO.1					X	
FPR_PSE.1						X

Table 32: TOE Security Functions/SFRs mapping

[145] The following table provides a rationale for the mapping between the TOE’s SFRs and the Security Functions.

SFR	SF and rationale
FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_SAR.2 FAU_SAR.3 FDP_IFC.1 FDP_IFF.1	<p>SECURITY AUDIT - The TOE generates the log of the operations performed by TOE users according to the events categories specified in the Table 30: Category of Security Relevant Auditable Events for Administrative profile and in the Table 31: Category of Security relevant Auditable Events for USR profile</p> <p>The TOE associates the identity of the user that caused the event for each event logged.</p> <p>Through the Dashboard SAM/ADM and authorized ADR administrators can view and audit the log of the operations perform by TOE users.</p> <p>Beside each USR user can view and audit the log of the operations performed, on files he owns, both by himself and by other users to whom those files have been shared.</p> <p>Audit information are stored encrypted in the DBMS, thus their confidentiality and integrity are protected.</p>
FIA_UID.2 FIA_UAU.2 FIA_UAU.5 FIA_AFL.1 FIA_SOS.1 FIA_ATD.1	<p>IDENTIFICATION AND AUTHENTICATION – The TSF requires users to identify and strongly authenticate themselves before invoking any other TSF function or before viewing any TSF data. No action can be initiated before proper identification and strong authentication providing a valid One Time Password (together with username and password) to access BBOP.</p> <p>After three consecutive failed authentication attempts the TOE requires to insert a captcha code and for each wrong captcha code inserted the TOE introduces an increasing delay before asking to insert the next captcha code.</p> <p>The TSF provides a mechanism to verify passwords meet at least eight characters, at least one number, at least one lowercase letter and at least one uppercase letter.</p> <p>The TSF maintain a set of security attributes for individual users that are used to enforce the TOE security policies.</p>
FDP_ACC.1 FDP_ACF.1 FMT_SMR.1 FIA_SOS.1 FPR_UNO.1	<p>ACCESS CONTROL – The users shall access to BBOP providing a valid username, password and OTP. TOE users are granted access to TOE functionalities according to their role and permissions set at their creation time by authorized administrators. Access to uploaded data (file) is granted to data owner, to TOE users according to the file sharing template and, in case the file is classified, to the TOE users that are member of the classification project.</p> <p>When a PERSONAL KEY is defined to access a file or the files belonging to a classification project, the personal key must satisfy the same complex criteria defined for passwords.</p> <p>Deter Photoshots Protection can be defined by an authorized user on the files he shares. This anti-capture option can make external users to display only a portion at a time of shared files to prevent that an unauthorized user captures the entire user data displayed on the screen.</p>

SFR	SF and rationale
<p>FPT_TEE.1</p> <p>FMT_SMF.1</p> <p>FMT_MTD.1 FMT_MOF.1</p> <p>FMT_SMR.1</p> <p>FMT_MSA.1 FMT_MSA.3 FDP_ACC.1 FDP_ACF.1</p>	<p>SECURITY MANAGEMENT – The TOE during its installation provides a set of tests to check the connectivity and the correct configuration of storage systems and DBMS with which it interfaces.</p> <p>The management functions that must be provided for effective management of the TOE through the Dashboard and the Control Panel are defined and described.</p> <p>The Administrator role and permissions determine the ability to use TOE security functions through the Dashboard.</p> <p>The TOE provides the roles specified in FMT_SMR.1 SFR. When a TOE user is created or modified, the role is specified by setting or clearing the administrative or user settings.</p> <p>The TOE ensures the access and management of the security attributes are restricted to specific roles as to enforce the TOE access control policies.</p> <p>The TOE ensures the default values of security attributes are permissive in nature as to enforce the TOE access control policies.</p>
<p>FPT_TEE.1</p> <p>FDP_IFF.1 FDP_IFC.1</p> <p>FDP_ETC.1 FDP_ETC.2 FDP_ITC.1 FDP_ITC.2 FDP_UCT.1 FDP_UIT.1 FPT_TDC.1</p>	<p>USER DATA and TSF DATA protection – The TOE during its installation provides a set of tests to check the connectivity and the correct configuration of storage systems and DBMS with which it interfaces.</p> <p>The TOE with the support of its operational environment forces encryption of all user personal information, user files (uploaded data) and email messages, as well as TOE Master Key, TOE configurations, TOE users’ credentials, AUDIT log files, sharing templates and SHA-256 hashes of uploaded data, needed to check their integrity before download.</p> <p>The encrypted user files are sent to the storage system by the TOE according to a specific set of rules that guarantee the correct encryption by the operational environment and subsequent interpretation and integrity check, while the other USER DATA and TSF DATA are stored encrypted in the DBMS.</p> <p>The TOE protects the USER data from disclosure and modification when it is transmitted outside the TOE.</p> <p>When the user file is imported from the storage system or from the DB the TOE, with the support of TOE operational environment, ensures the correct interpretation of it’s hash which is used by the TOE to detect any random changes occurred during the permanence of the files on the storage system or on the DB.</p>
<p>FPR_PSE.1</p>	<p>PRIVACY – during data upload TOE users pseudonymity is granted by aliases defined for them.</p>

Table 33: SFR to TSF rationale