Boole Server Security Target Ver. 1.5

REVISION HYSTORY

Version	Modification Date	Description of changes
1.5	**2015-10-05**	**First public Issue**

TABLES OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

REFERENCES

[CCP1] CCMB-2012-09-001 - Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, ver. 3.1 Revision 4, September 2012.

[CCP2] CCMB-2012-09-002 - Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, ver. 3.1 Revision 4, September 2012.

[CCP3] CCMB-2012-09-003 - Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, ver. 3.1 Revision 4, September 2012.

[CEM] CCMB-2012-09-004 - Common Methodology for Information Technology Security Evaluation - Evaluation Methodology, ver. 3.1 Revision 4, September 2012.

[RC6] The RC6 Block Cipher – Ronald L.Rivest, M.J.B Robshaw, R. Sidney and Y.L. Yin, Version 1.1 – August 20, 1998.

DOCUMENT TERMINOLOGY

TERM	DEFINITION
CC	Common Criteria (ISO/IEC 15408) Version 3.1 Rev. 4
EAL	Evaluation Assurance Level
IT	Information Technology
ISP	Internet Service Provider
OS	Operating System
OSP	Organizational Security Policy
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation. In the following chapters Target of Evaluation (TOE) stands for the Boole Server.
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functionality Interfaces
GAM	General Administrator Master role
GAR	General Administrator Restricted role
PU	Power User role
SU	Super User role
GrA	Group Administrator role
U	User role
G	Guest role
Passphrase	Alphanumeric string of variable length used by the TOE during generation of RC6 key

Table 1: Terms and Acronyms used in Security Target

1 ST INTRODUCTION

1.1. ST REFERENCE

[1]

Title:	*Boole Server Security Target*
Version:	*1.5*
Date:	*5th October 2015*
Assurance Level:	*EAL 2 augmented with ALC_FLR.2*
CC Version:	*Common Criteria v.3.1 Revision 4*
Author:	*Boole Server S.r.l.*

Table 2: ST Reference

1.2. TOE REFERENCE

[2]

Server Side	*Boole Server version 3.2*
Agent	*Boole Server Agent version 3.2*
Web Client	*Boole Server Web Client version 3.2*

Table 3: TOE Reference

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 4: 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. 4 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, i.e. *assignment_value(s).*
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by *underlined italicized* text.
- 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.

[5] Italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5. TOE OVERVIEW

[6] **Information Centric Security:** In today's fast moving business world, organizations need to share sensitive information across the internal organization and to third parties outside such as customers, partners and the supply chain. The challenge for customers wanting to address this requirement in a secure manner frequently takes two forms.

[7] **Sharing vs Security**
Normally security and collaboration are considered mutually conflicting goals. The more secure you become the more "uptight" you need to be about sharing information; the more collaborative you need to become the more you need to "let down your guard". This problem is particularly obvious when information is unstructured and in the form of documents, reports, emails, images and drawings.

[8] **Current security investments do not address the problem**
Traditionally information security takes the form of securing computers, networks and people to whom information can or cannot flow. This is done by creating "perimeter" defense and constraining information to only flow freely within this perimeter and not-so-freely across the perimeter.
However, existing information security investments within customers do not cater for ensuring that sensitive files remain secure and under the control of the data owner after they have been shared. Up until now, the very act of sharing a file with another person means that you lose control over what happens to it once it has been sent.

[9] Boole Server allows enterprises to achieve the "mutually conflicting" goals of security and collaboration by breaking down traditional tenets of information security via distribution control.

1.5.1. USAGE AND MAJOR SECURITY FEATURES OF THE TOE

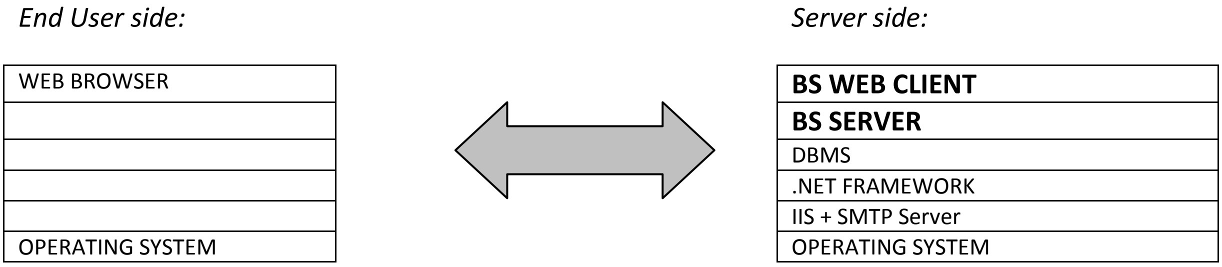
[10] Boole Server is a secure, scalable system designed to safeguard sensitive data, while allowing it to be shared with staff, partners and customers as and when needed.
Boole Server ensures that data cannot be lost or stolen when in transit or on the server and that only authorized recipients can use, edit or view specific files.

[11] Boole Server 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 Boole Server 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.

[12] Boole Server empowers organizations to choose how they store and share confidential information. The solution enables secure centralized collaboration and also the capability to protect data locally, while still enforcing security even after the file has been shared via e-mail, CD, USB, etc.

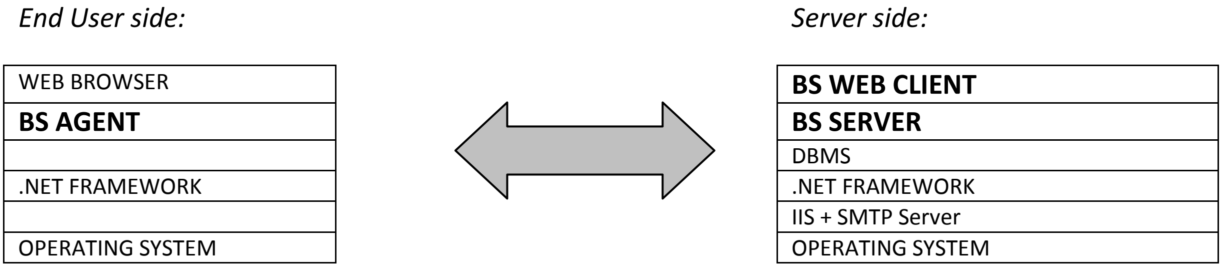
[13] The TOE can be used in two different configurations as shown below (in BOLD are represented the TOE components):

CONFIGURATION 1:



End User side:	*Server side:*
WEB BROWSER	**BS WEB CLIENT**
	BS SERVER
	DBMS
	.NET FRAMEWORK
	IIS + SMTP Server
OPERATING SYSTEM	OPERATING SYSTEM

CONFIGURATION 2:



End User side:	*Server side:*
WEB BROWSER	**BS WEB CLIENT**
BS AGENT	**BS SERVER**
	DBMS
.NET FRAMEWORK	.NET FRAMEWORK
	IIS + SMTP Server
OPERATING SYSTEM	OPERATING SYSTEM

[14] The difference between the two configuration is the presence or absence of the Boole Agent represented in configuration n° 2. This configuration provides a greater level of control and protection compared to configuration 1. As described in details below, Agent users are able to encrypt files and folders stored locally, create encrypted local disks, block screen-capture activities, encrypt local resources making them accessible even without connection to the Boole Server and much more.
When the end user side does not have the ability to connect to the server the BS Agent allows to access and use protected files or archives by using an offline certificate previously generated.

1.5.2. TOE TYPE

[15] The TOE is composed of three software components, developed with Visual Studio 2010:

- Server component (indicated in the following as *Boole Server* or, simply, BS *server*)
- Agent component (indicated in the following as *Boole Agent* or, simply, BS *agent*)
- Web Client component (indicated in the following as *Boole Server Web Client or, simply BS Web Client*)

[16] The TOE can be viewed as covering to the following categories

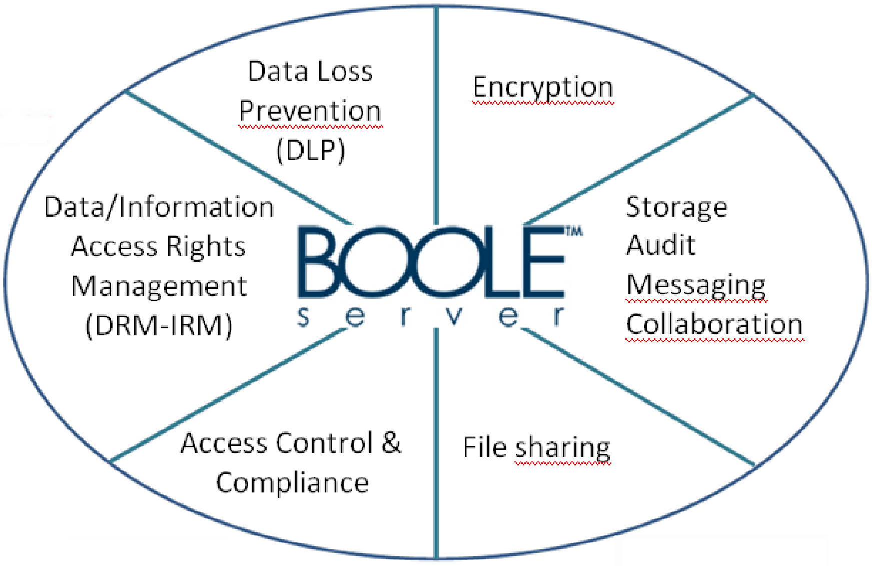

Data Loss Prevention (DLP)
Encryption
Data/Information Access Rights Management (DRM-IRM)
BOOLE™ server
Storage
Audit
Messaging
Collaboration
Access Control & Compliance
File sharing

Figure 1: Product categories covered by Boole Server

1.5.3. REQUIRED NON-TOE HARDWARE/SOFTWARE

1.5.3.1. SERVER SIDE

Operating System	Microsoft Windows Server 2012 Microsoft Windows Server 2008R2
Minimum Software Prerequisites	Following versions of Microsoft DBMS: • SQL Server 2012 • SQL Server 2008R2
	.NET Framework 4.0
	IIS (Internet Information Server) 6
	Microsoft Office 2007
Minimum Hardware Prerequisites	**Ram**: 4 GB
	Disk Space: 1 GB
	Network Card: 10/100 Mbit
	CPU: Dual Core Processor

Table 5: Minimum SW and HW prerequisites of Server and Web Client components

1.5.3.2. END USER SIDE

Operating System	Following versions of Microsoft Windows OS: • Microsoft Windows 8 e 8.1 • Microsoft Windows Server 2008 (all versions) • Windows 7 • Windows Vista
Software Prerequisites	Microsoft Internet Explorer (from version 7 and up) All other major internet browser (Chrome, Safari, Opera, Firefox) *Note*: Browsers HTML 5 compliant in their most updated version recommended
	.NET FRAMEWORK V 3.5 (*Note*: only with TOE configuration n. 2)
Hardware Prerequisites	PC with at least the minimum hardware required by the operating system

Table 6: Software prerequisites of Agent component

1.6. TOE DESCRIPTION

[17] Boole Server installed in customer's infrastructure allows to centrally manage all user access and rights to access the protected data and, in addition, to set all system configurations for the infrastructure in which it is located Boole Server from the control panel available.

[18] Boole Server allows data protection in two different way:

- ***Encryption of files contained in any storage unit***: the encrypted files will have the same path of the original ones and then they can be exchanged using any of the means actually known (e.g. Email, file sharing, etc.)
- ***Centralization of files into the storage configured in Boole Server***: it is possible to upload and share files in Boole Server storage using the Web Client application, in a way similar to the one offered by most popular online storage services as DropBox, Microsoft OneDrive with the fundamental difference that Boole Server data are stored in encrypted mode in the internal storage of the customer company and not at an external ISP premises: for this reason, during initial configuration phase, Boole Server prompts to define a storage unit.
  The centralized data protection system enables IT professionals, companies and individuals to use the files from the outside connecting with each kind of device (tablet, smartphone, laptop) in security. The platform is able to encrypt and protect sensitive data from any attempt to copy, theft, tampering or unauthorized interception.

[19] In the following paragraphs the main security characteristics of Boole Server are summarized:

[20] PERSISTENT ENCRYPTION: Boole Server secures file, e-mail and text using a 2040 bit encryption key, based on the RC6-32/20 symmetric algorithm.
To ensure the confidentiality of information protected by Boole Server, the decryption keys are stored centrally in Boole Server database and not in the same place with the file itself, so they are never exposed. The encryption/decryption keys are randomly generated for each different connections and for each file and stored. The random generation functionality (RNG) is provided by the operational environment (Microsoft .Net CNG - Cryptography API: Next Generation) Features). As a result files cannot be decrypted without the information owner's authorization via Boole server. Furthermore, the protection applied by Boole Sever continues even when encrypted files are in use, unlike other encryption systems whose protection disappears when files are decrypted and read, Boole Server offers persistent protection even after files are opened by a user. Under particular conditions Boole Server protects file contents even when viewed in clear for example from screenshot, video grabbing, copy and paste, malware copying files being used on the personal computer.

[21] **FLEXIBLE ACCESS:** Boole Server users have the ability to access protected information from anywhere and at anytime 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 Boole Server for each operation required.
Boole Server provides a framework to define the appropriate access rights to a file, for example:

- WHO can use the information i.e. people / groups within or outside of the enterprise
- WHAT can each person do with the information i.e. read / edit / print / distribute / copy / watermark / Secure download PDF / Saving to .BS3
- WHEN can each person access the information i.e. within certain dates, within a time span in seconds
- WHERE can the information be accessed from i.e. specific IP address, within the office

[22] Using Boole Server it is possible to create a Secure Cloud within an organization over the SSL communication protocol (the same standard globally adopted in the financial industry).

[23] **ABSOLUTE PROTECTION:**
Boole Server's innovative approach to information protection has a far wider scope than the limited solution of perimeter security.
Boole Server's protection is not based on the premise that data is used either inside or outside of the company: with Boole Server, files are protected everywhere and all the time.

[24] Importantly, Boole Server's architecture ensures that system administrators are not able to use their privileges to access the content of protected files; only 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 attached 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.

[25] 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 user assignment groups.

[26] Protection rules define the action taken when an attempt is made to transfer or transmit tagged data. The protection rule specifies the transfer method, named tag(s), and how the system should react to the event. Each event is given a severity level, and options for responding to the event. In some cases, protection rules merely log the event. In other cases, the protection rules may prevent the transfer of data and notify the user of the violation. Protection rules are optionally applied to assignment groups. This allows a rule to apply only to particular user groups.

[27] **AUDITING:** Boole Server's advanced Auditing system ensures complete knowledge of all activity within the system. The data manager can see a clear visual report of all the activities that have been carried out on a given file and track which operations have been performed by any given user. Boole Server is able to audit the usage of the information providing a complete secured record of WHO used the information, WHAT was being done, WHEN and WHERE the action is captured in the collaboration environment.

[28] **SECURE SHARING:** Boole Server 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.
Boole Server's Granular and Dynamic Rights Management, allows real time editing of any users 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 transferred via the Client or emailed to the recipient as an attachment. Once delivered, the correct file access policy is applied according to the latest version; ensuring appropriate access is always maintained.
- Protect the network by blocking access to a specific list or range of IP addresses. All requests outside these parameters will be denied access to the server.
- Close all unused ports since all services provided by Boole Server use a single communication port.
- Protects the network thanks to the proprietary encryption used for data management. Data transferred is encrypted, as a result any intercepted data is impossible to view.

[29] **REMOTE DRIVE:** The Remote Drive functionality allows a profile to access a specific directory in the local sources from remote. Thanks to this option, any change performed in the specified directory will automatically be synchronized both in local and in Boole Server, regardless the fact that the change was made in the local disc or by a Boole Server Web Client.
By performing a connection through a client, this functionality makes it possible to have the contents of a directory shared in local through i.e. Microsoft Active Directory from remote.

1.6.1. Boole Server Architecture

[30] **SERVER**

Boole Server is a security platform designed to protect against unauthorized viewing, manipulation or distribution of confidential data.
The Server component is the core of the protection architecture and manages all operations. The Server 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 Boole Server to focus on:

- control of data confidentiality
- protection of intellectual property
- customizable rights with differentiated access to information according to functional and hierarchical role
- audit of the operations that users perform on files.

[31] **AGENT**
The Agent provides an even greater level of control and protection. Agent users are able to:

- Block Screen-capture activities, such as screen shot and video streaming
- Work on files while they are protected
- Encrypt files and folders stored locally
- Share locally encrypted files with dynamic granular rights management
- Revoke access rights at any time
- Create encrypted local disks
- Synchronize a local disk with the centralized resources through the Web Client
- Encrypt local resources making them accessible even without connection to the Boole Server.

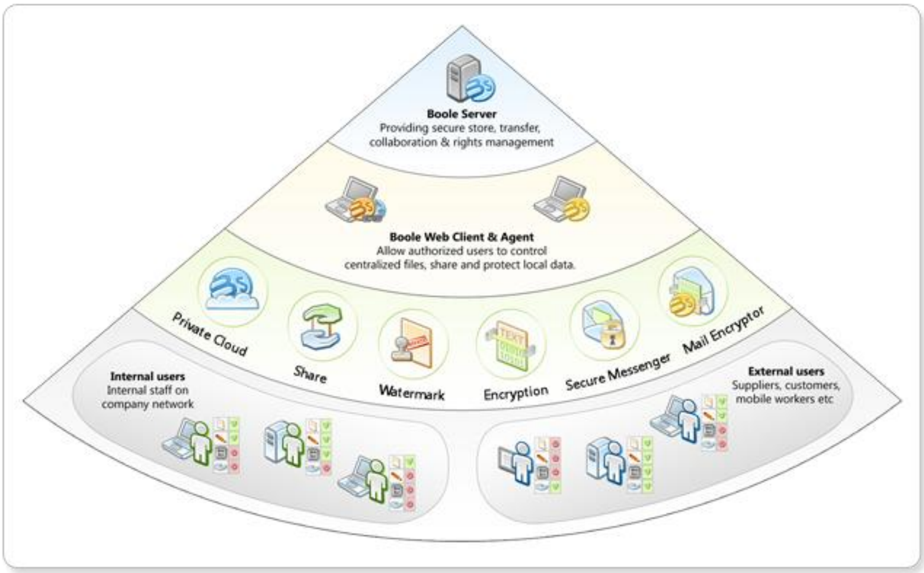

Boole Server
Providing secure store, transfer, collaboration & rights management
Boole Web Client & Agent
Allow authorized users to control centralized files, share and protect local data.
Private Cloud
Share
Watermark
Encryption
Secure Messenger
Mail Encryptor
Internal users
Internal staff on company network
External users
Suppliers, customers, mobile workers etc

Figure 2: Boole Server High Level Architecture

[32] **WEB CLIENT**

[33] Users are able to access all the functionality of Boole Server via any internet browser.

[34] Through the Web Client control panel it is possible to:

- Centrally store and protect files and folders
- Share information in a granular and temporary way
- Create and control access profile
- Monitor the activities performed by users on protected information
- Send and receive encrypted messages
- View files in protected mode
- Encrypt text
- e-mail direct links to access centralized protected information.

1.6.2. Typical usage of Boole Server within customer infrastructure architecture

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

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

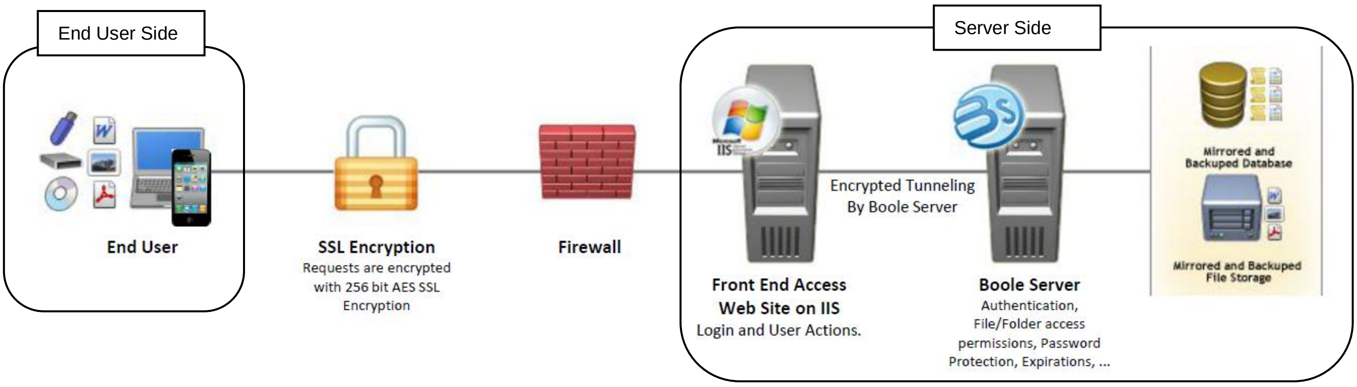

End User Side
End User
SSL Encryption
Requests are encrypted with 256 bit AES SSL Encryption
Firewall
Server Side
Encrypted Tunneling By Boole Server
Front End Access Web Site on IIS
Login and User Actions.
Boole Server
Authentication, File/Folder access permissions, Password Protection, Expirations, ...
Mirrored and Backuped Database
Mirrored and Backuped File Storage

Figure 3: Typical usage of Boole Server within customer infrastructure architecture

[37] Typical HA infrastructures reference scenarios are:

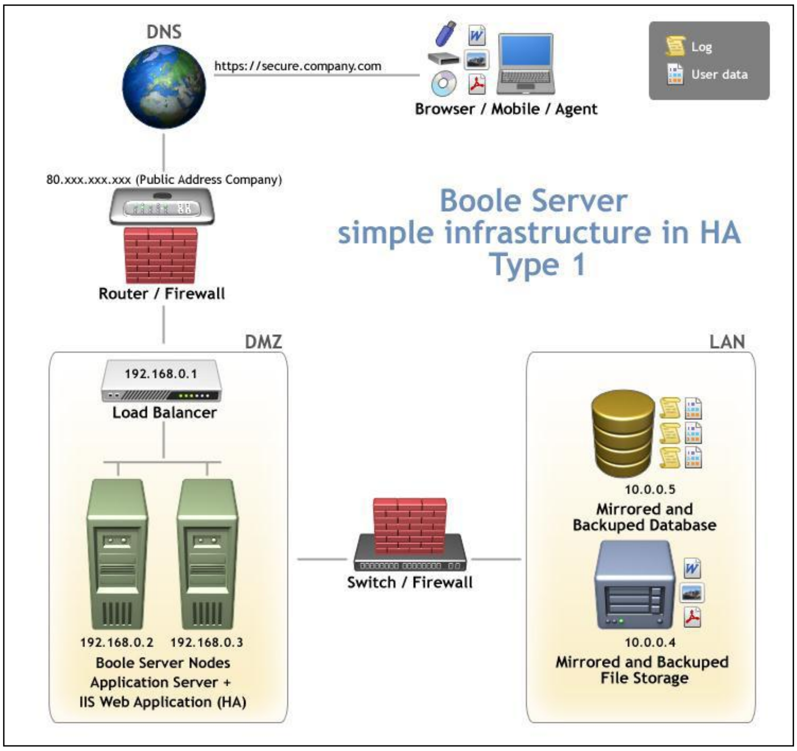


Figure 4: Example of Boole Server usage in simple infrastructure in HA – type 1

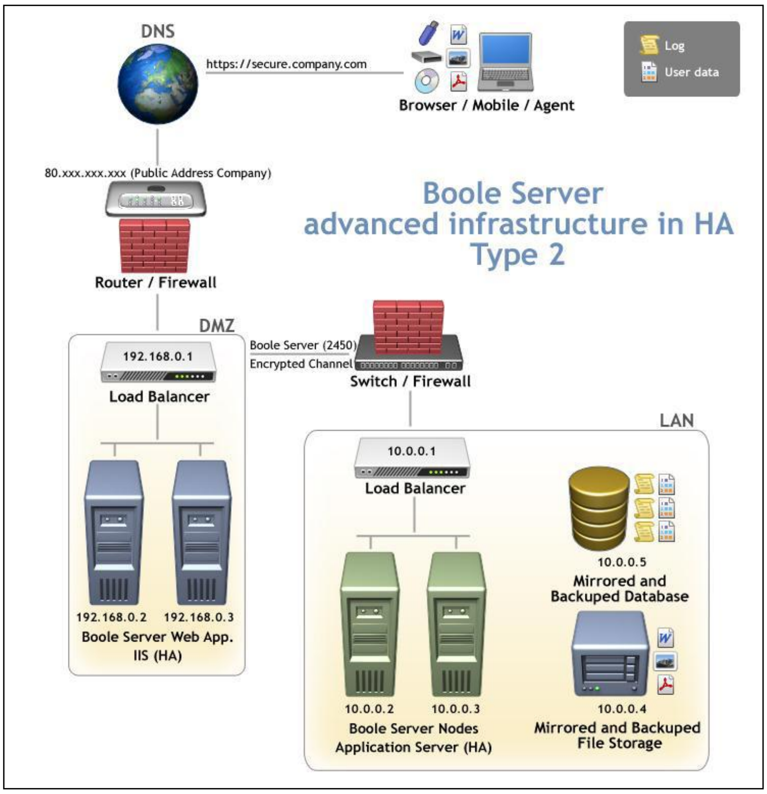


Figure 5: Example of Boole Server usage in simple infrastructure in HA – type 2

1.6.3. Boole Server users profiles

[38] This section shows the user profiles that can be defined both server side and client side: the "server side user profiles" are all the profiles that can be created and managed by the component BS Server while the "client side user profiles" are all the profiles that can be created and managed by the component BS Web Client.

[39] A major difference between the two kind of profiles is that the server-side user profiles are created during installation of Boole Server and can be managed only by local administrative user.
User profiles on the client side can also be managed remotely via the web interface of the component BS Web Client.

1.6.3.1.Boole Server users profiles – SERVER SIDE

[40] **General Administrator Master (GAM)**

[41] The General Administrator Master role is the first one created and it must be defined during Boole Server installation.
A user with the GAM role has full access rights to all TOE's features and is authorized to edit all the settings available on the Boole Server application.
Only the GAM , i.e. who installs Boole Server can create, at server side, and edit in complete freedom each kind of user profiles authorized to access data.
Only the GAM is allowed to define, manage and delete a General Administrator Restricted (GAR) role, i.e. a General Administrator with limited right versus a General Administrator Master.
The GAM defines the REDKEY , the symmetric key needed to encrypt the whole Boole Server database, defined at TOE installation time and that can be changed in any moment during TOE lifetime.
The credentials of this administrator together with the security REDKEY and a specific configuration file are also needed to recover data following a disaster or to restore a previous installation of TOE.
The GAM is allowed to enable or disable the System log that is a log file of all events and malfunctions processed by the BS Server;
The GAM is allowed to set Users log period that is a log file of all operations performed by any Boole Server end users that it's stored encrypted in the database;
The GAM is allowed to view the logs of its operations and those made by the GAM and Power User only using the REDKEY .
The GAM is allowed to create, modify and delete the Group Administrator profile (GrA).
The GAM is authorized to create and delete Boole Server groups and profiles.
The GAM may limit the number of operations that the GAR can perform. Thanks to this option, the control on the activities performed by GAR will be even more strict and controlled and the limitation of the number of allowed actions is the same as making a double authorization for each server side-performed operation.
The GAM defines the BS Server parameters: General Administrator parameters, Boole Server Groups parameters, Server setup parameters, Advanced Identity Platform parameters, Storage parameters, Database parameters, SMTP server parameters, Boole Server Farm parameters, Remote Drive parameters, Options parameters.
The GAM is allowed to set timetables restriction to access the TOE for profiles belonging to all groups;
In any case the GAM is not allowed to access the user data.

[42] **General Administrator Restricted (GAR)**

[43] The General Administrator Restricted is allowed to create a GAR having its own privileges.
The main difference is that the GAR cannot install BS server, cannot restore BS server and delete the account of the GAM.

[44] **Power User (PU)**

[45] The purpose of this user is to "view". He is allowed to view the structure of groups and the user data but he is not allowed to modify anything.

1.6.3.2.Boole Server users profiles – END USER SIDE

[46] **Super User (SU)**
The Super User is created by a General Administrator (GAM/GAR) and he is allowed to create Group Administrators as well as he is allowed to manage crosswise the users belonging to created groups.
At his creation Super User is associated with a *dummy* group.
The Super User is allowed to access the functions for auditing all the groups he managed only if the GAM or GAR has granted this privilege.
The Super User is allowed to use the following functionalities: Profile Manager, Auditing, change PIN, Alias Management functions and change Advanced Identity Platform parameters.
Only Super Users is allowed to create new profiles within different Boole Server groups;
Only Administrators can be allowed to remove sharing to a profile belonging to their group but in general only those who have made a share can remove it. Super Users are not allowed to access protected files or text, both centralized and local. Super Users can be created server-side only. The Super User is allowed to create the Group Administrator (GrA) using the BS Web Client Panel.

[47] **Groups Administrator (GrA)**
The *Group Administrator role* can administer (with limited abilities compared to the *General Administrator*) groups of users using Boole Server Web Client component.
Note that from Boole Server point of view, each group has its own Group Administrator.
The GrA is allowed to use the following functionalities if privilege was granted by GAM/GAR/SU:
File Manager, Profile Manager, Auditing and Secure Messenger, change PIN, Alias Management functions and change Advanced Identity Platform parameters.
The GrA is not allowed to create groups but only users.

[48] **User (U)**
A *Users role* can access to BS Web Client and depending on the privilege granted by GrA can use the Secure Messenger or File Manager.
User profile disposes of some space for centralized storage of files (using Boole Server Web Client) and is enabled to encrypt files and text in local (using Boole Server Agent).

[49] **Guest (G)**
Guest profile does not dispose of any space for centralized storage of files and is not allowed to encrypt text or files, but is enabled to access the shared resources (centralized files, encrypted text or files) they have received, according to the privileges they have been given.

1.6.4. PHYSICAL SCOPE OF THE TOE

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

- Boole Server Version 3.2;
- Boole Server Agent Version 3.2;
- Boole Server Web Client Version 3.2;

[51] In the following figure are represented the TOE components in each TOE configuration allowed:

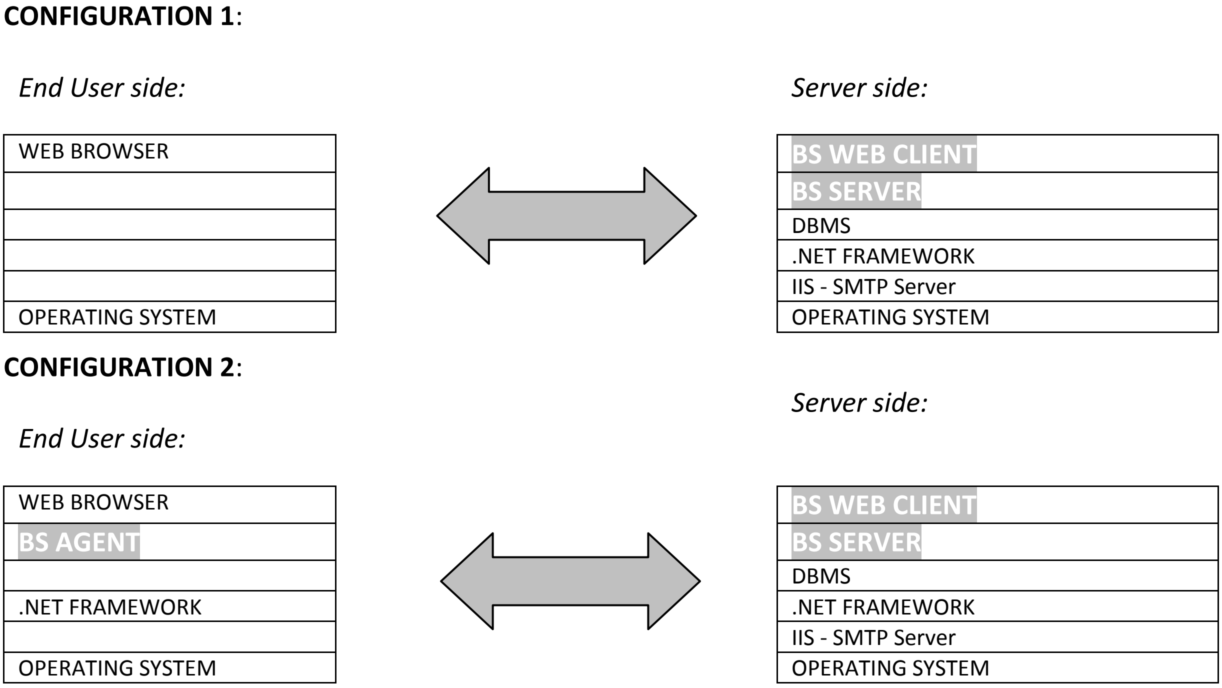


Figure 6: TOE boundary

1.6.5. LOGICAL SCOPE OF THE TOE

[52] This section outlines the logical boundary of the TOE which includes the security functionalities described in the following sections.

TSF	DESCRIPTION
Security Audit	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. According to what has been defined by GAM/GAR/SU roles, each operation performed by GAR/SU/GrA respectively is logged by Boole Server and can be audited according to auditing filters defined. Logs are stored encrypted in the DBMS. GAM/GAR logs can be viewed from server side by accessing the panel provided by Boole Server locally, i.e. where BS Server resides (BS local panel) and using the REDKEY . SU/GrA logs can be viewed by accessing the BS web Client panel.
Identification and authentication	The Identification and Authentication TSF ensures that only legitimate administrators can gain access to the configuration settings and management settings of the TOE. End users must log in with a valid user name, PIN and Group membership before the server will permit them to access the TOE. If the *Enable Strong Authentication* option is set (only for end user) the TOE users must be strongly authenticated via an additional OTP password before they can be granted to access stored data. Server side users must log in with a valid user name and password before the server will permit the administrators to manage the TOE.
User data protection	Using Boole Server, 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.
Security Management	The TOE provides a set of commands for authorized users to manage the security functions, configuration, and other features of the Boole Server. The Security Management function specifies user roles with defined access for the management of the TOE components. 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.
Cryptographic Support	By default, the Boole Server encrypt all file using RC6 2040 bit keys. This ensures sensitive data can only be viewed and used by authorized users, without the risk of critical information being unduly intercepted
Communication	BS server protects the communication between itself and the End user when the TOE is in configuration 2.

Table 7: Logical Boundary descriptions

1.6.6. TOE Guidance Documentation

[53] The following guidance documentation is provided as part of the TOE:

- Boole Server Installation Guide
- Boole Server Administration Guide
- Boole Server User Guide

2 CONFORMANCE CLAIM

2.1. CC CONFORMANCE CLAIM

[54] This Security Target and this TOE are conform to Common Criteria version 3.1 rev. 4.

[55] In particular, this Security Target is compliant with:

- Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, conformant, ver. 3.1 Revision 4, September 2012, CCMB-2012-09-002
- Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, conformant, ver. 3.1 Revision 4, September 2012, cod. CCMB-2012-09-003 at Evaluation Assurance Level 2 augmented with ALC_FLR.2.

2.2. PP CONFORMANCE CLAIM

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

3 SECURITY PROBLEM DEFINITION

[57] This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed.

[58] In order 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 manner in which the TOE is intended to be used.

[59] This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1. THREATS

[60] The following table lists the threats.

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

Threat	*Description*
T.INTEGRITY	An unauthorized user may compromise the integrity of the data generated or stored by the TOE bypassing a security mechanism.
T.INTERCEPT	A subject 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 configuration of the TOE, intentionally or not, causing potential intrusions to go undetected.
T.FUNC	An unauthorized user may obtain access to the TOE to modify the TOE security functions.
T.SCREEN	An unauthorized user may stole 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.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.KEY_ACCESS	An user or process may cause key, data or executable code associated with the cryptographic functionality 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 cryptographic keys due to weak keys generated by the TOE's key generation mechanisms.
T.INSTALL	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.MASQUERADE	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.

Threat	*Description*
T.FILL_RECORDS	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.CRASH	A system failure or system crash makes unusable the current installation of the TOE.
T.INTERR	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 failures of software, hardware, power supplies, or storage media.

Table 8: Threats

3.2. ORGANISATIONAL SECURITY POLICIES

[62] An organizational security policy is a set of rules, practices, and procedures intended to be imposed by an organization using Boole Server 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.

Policy	*Description*
P.ACCOUNT	Users of the TOE shall be accountable for all their activities and 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	All data collected and produced by the TOE shall only be used for authorized purposes.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from unauthorized modification.
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	SO and DBMS Administrators must ensure that audit facilities are used and managed effectively. These procedures shall apply to the TOE's audit trail and the audit trail for the underlying operating system and the database servers and/or secure network services. In particular: 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 9: Organizational Security Policies

3.3. ASSUMPTIONS

[63] 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.

Assumption	*Description*
A.TRAINING	It is assumed that users of the TOE will be trained sufficiently in order to operate the TOE.
A.DBMS_ACCESS	It is assumed that the DBMS is installed in the TOE environment and that the physical and logical 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.STORAGE_ACCESS	It is assumed that the Storage is installed in the TOE environment and that the physical and logical 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.ALIGNEDBACKUPS	It is Assumed that BS server, DBMS and Storage in TOE environment are regularly backuped in a way that grants that the backups are kept aligned.
A.TRUST	It is assumed that the authorized administrators are not hostile, careless or willfully negligent observing the instructions provided by the TOE documentation.
A.TIME	It is assumed that the operational environment provides a reliable time reference.
A.SECCOMM	It is assumed that the IT environment will provide a secure line of communication between distributed portions of the TOE and between the TOE and remote administrators.
A.TOE_EVALUATED	The TOE is installed, configured, and managed in accordance with its evaluated configuration.
A.USERS	It is assumed that authorized users do not actively or negligently compromise the security of the computer on which the TOE is installed. Examples for such compromising actions would be: - Placing malicious software (like programs containing viruses or Trojan horses) on the computer, - modifying the TOE program or data files.
A.RESTRICT	The OS upon which the TOE resides will be configured to restrict modification to TOE executables, the OS itself, configuration files, databases and passphrases to only the authorized administrators. (This is in order to prevent unauthorized changes concerning the platform as well as the TOE and its configuration.)
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 have to be removed (e.g. by installing corresponding hot fixes) or protected by appropriate external security measures.
A.REDKEY	It is assumed that IT environment ensures that the REDKEY is kept in a safe place under control of the General Administrator Master.
A.BACKUP	It is assumed that the IT environment ensures that the DB and STORAGE are securely backuped.
A.INTEGRITY	It is assumed that the operation environment ensure the integrity protection of the executable files constituting the TOE.

Table 10: Assumptions

4 SECURITY OBJECTIVE

[64] 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

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

Objective	*Description*
O.AUDIT	The TOE must: - record audit records upon data accesses and use of the TOE functions on the management system; - make available audit tools to assist authorized users in the review of audit data.
O.AUDIT_PROT	The TOE shall protect the integrity, confidentiality and availability of audit information generated by itself.
O.ACCESS	The TOE shall allow authorized users to access only to authorized TOE functions and data.
O.MANAGE	The TOE shall include a set of functions that allows the efficacious management of its functionality and data.
O.IDENTIFY	The TOE shall identify users prior to allowing access to its functions and data.
O.CONFIDENTIAL	The TOE shall protect the confidentiality of the user data when displayed.
O.CRYPTO	The TOE shall encrypt the files before storing them, according to the owner's user profile.
O.INTEGRITY	The TOE must ensure the integrity of all TOE data.
O.CRASH	The TOE shall permit to recover its configuration in event to disaster or to restore its previous installation.
O.ANTI_BRUTE	The TOE shall take specified actions to disable the account of the user that attempts to guess the BS Web-Client PIN with brute force attack.
O.STRONG_KEYS	The TOE shall generate strong cryptographic keys to withstand an attack that attempts to guess the key.
O.CONFIG	The TOE, during the installation, shall ensure the presence of required software.
O.OTP	The TOE shall implement a mechanism for authentication based on One Time Password (OTP).

Table 11: Security Objectives for the TOE

4.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

[66] The operational environment of the TOE implements technical and procedural measures to assist the TOE in correctly providing its security functionality.

[67] In the following table are described a set of statements describing the goals that the operational environment should achieve.

Objective	*Description*
OE.TIME	The operational environment shall provide a reliable time reference.
OE.CRYPTO	The operational environment shall provide cryptographic functionality (RSA 512 bit key generation, Random Number Generation, RSA encryption/decryption) and protocols (HTTPS based on AES256) to properly support the TOE for secure transfer of information as detailed below: - between End User side and Server Side and separate parts of the TOE (BS Server and BS Web Client) when the TOE is in configuration 1; - between separate parts of the TOE (BS Server and BS Agent) when the TOE is in configuration 2.
OE.AUDIT_PROTECT	The operational environment shall provide the capability to protect the integrity of audit log files generated by the TOE via mechanisms outside the TSF.
OE.STAFF	Staff working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE and proper TOE configuration at installation phase.
OE.DB	Those responsible for the TOE configuration and administration must ensure that physical and logical access to the DBMS in TOE environment via mechanisms outside the TOE boundary is restricted to authorized administrative users only.
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 authorized administrative users only.
OE.BACKUP	The operational environment shall provide a secure back-up of DBMS and Storage data.
OE.CONTINUITY	The operational environment shall provide a system to ensure operational continuity in the event of a power failure.
OE.LOG_STORE	The operating environment shall provide a system capable of storing at least 120 days of logs.
OE.INTEGRITY	The operational environment shall provide the capability to protect the integrity of executable files of the TOE using .NET framework technology.

Table 12: Security objectives for the operational environment

4.3. SECURITY OBJECTIVES RATIONALE

[68] 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/	O.AUDIT	O.AUDIT_PROT	O.ACCESS	O.MANAGE	O.IDENTIFY	O.CONFIDENTIAL	O.CRYPTO	O.CRASH	O.ANTI_BRUTE	O.STRONG_KEYS	O.CONFIG	O.OTP	O.INTEGRITY	OE.TIME	OE.LOG_STORE	OE.CRYPTO	OE.CONTINUITY	OE.AUDIT_PROTECT	OE.STAFF	OE.BACKUP	OE.DB	OE.STORAGE	OE.INTEGRITY
T.DISCLOSE			▨		▨																		
T.INTEGRITY		▨	▨		▨								▨					▨					
T.INTERCEPT							▨			▨						▨							
T.CONFIG			▨	▨	▨																		
T.FUNC			▨		▨																		
T.SCREEN						▨																	
T.NOTRACE	▨	▨	▨		▨									▨				▨					
T.INSTALL											▨								▨				
T.BRUTE									▨														
T.MASQUERADE												▨				▨							
T.FILL_RECORDS															▨								
T.CRASH								▨												▨			
T.INTERR																	▨		▨	▨			
T.KEY_ACCESS			▨		▨																▨		
T.KEY_GUESS										▨						▨							
T.LOSSOF			▨		▨								▨										
T. PRIVIL			▨		▨																		
P.ACCOUNT	▨				▨									▨									
P.PROTECT		▨	▨		▨		▨									▨		▨				▨	
P.MANAGE			▨		▨														▨				
P.ACCESS			▨		▨																▨		
P.FAILURE								▨									▨		▨	▨			
P.AUDITLOG														▨	▨			▨	▨				
P.INTEGRITY		▨	▨		▨		▨						▨			▨		▨			▨	▨	
A.TRAINING																			▨				

OBJECTIVE THREAT/POLICIES /ASSUMPTION/	O.AUDIT	O.AUDIT_PROT	O.ACCESS	O.MANAGE	O.IDENTIFY	O.CONFIDENTIAL	O.CRYPTO	O.CRASH	O.ANTI_BRUTE	O.STRONG_KEYS	O.CONFIG	O.OTP	O.INTEGRITY	OE.TIME	OE.LOG_STORE	OE.CRYPTO	OE.CONTINUITY	OE.AUDIT_PROTECT	OE.STAFF	OE.BACKUP	OE.DB	OE.STORAGE	OE.INTEGRITY
A.DBMS_ACCESS																					▨		
A.STORAGE_ACCESS																						▨	
A.ALIGNEDBACKUPS																				▨			
A.SECCOMM																▨							
A.TOE_EVALUATED																			▨				
A.USERS																			▨				
A.UPDATE																			▨				
A.RESTRICT																			▨				
A.REDKEY																			▨				
A.BACKUP																				▨			
A.TRUST																			▨				
A.INTEGRITY																							▨
A.TIME														▨									

Table 13: Tracing between security objectives for the TOE and security objectives for the Operational Environment vs Threat, OSP and Assumption

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

THREAT, POLICIES, ASSUMPTION	
T.DISCLOSE	An unauthorized user may reveal a data stored by the TOE bypassing a security mechanism. 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.
T.INTEGRITY	An unauthorized user may compromise the integrity of the data generated or stored by the TOE bypassing a security mechanism. 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. The O.INTEGRITY objective ensures no TOE data will be modified. O.AUDIT_PROT/OE.AUDIT_PROTECT specifically refer to audit data integrity grant by the TOE together with its environment.
T.INTERCEPT	A subject may intercept the data exchanged between a remote user and the TOE by sniffing the communication channel. The O.CRYPTO objective states that the TOE encrypts the files before storing them, according to the owner's user profile. The OE.CRYPTO provides cryptographic functionality and protocols required for the TOE to properly support the TOE for secure transfer of information between separate parts of the TOE (BS Server and BS Agent when the TOE is in configuration 2 and BS Server e BS Web Client when the TOE is in configuration 1). O.STRONG_KEYS objective provides strong cryptographic keys that increase the level of security communications between separate parts of the TOE.
T.CONFIG	An unauthorized user may change the configuration of the TOE, intentionally or not, causing potential intrusions to go undetected. 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. Beside, O.MANAGE provides a set of functions that allows the efficacious management of TOE functionality and data.
T.FUNC	An unauthorized user may obtain access to the TOE to modify the TOE security functions. 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.
T.SCREEN	An unauthorized user may stole reserved data by taking a screen shot or taking a picture of the data viewed on the monitor. O.CONFIDENTIAL protects the confidentiality of the user data when displayed.
T.NOTRACE	An unauthorized user may perform file operations bypassing or disabling the audit functions, i.e. without being accountable for it. 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.AUDIT objective implements this policy by requiring auditing of all data accesses and use of TOE functions. 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. 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. 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.
T.KEY_GUESS	An unauthorized user succeeds in guessing cryptographic keys due to weak keys generated by the TOE's key generation mechanisms. O.STRONG_KEYS objective refers to the ability of the TOE of providing strong cryptographic keys (255 byte long) by means of a proprietary algorithm starting from passphrases that, in some cases, are generated with the support of operational environment (.NET framework) that properly provides Random Number Generation functionality, as described in OE.CRYPTO, while in some other cases are known only by the TOE and protected by the TOE.

THREAT, POLICIES, ASSUMPTION	
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. 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.
T.KEY_ACCESS	An user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms. 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. OE.DB objective protects access to the DB in which the cryptographic keys are kept.
T.INSTALL	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms. O.CONFIG objective ensures, during the installation, the presence of software required for the operativity. OE.STAFF objective ensures that the staff working as authorized administrator is faithfully selected, skilled and trained for proper operation without compromising the TOE.
T.BRUTE	An unauthorized user that attempts to brute-force the web client authentication mechanism may go undetected. If the attacker is successful, TSF data may be lost or altered. O.ANTI_BRUTE objective provides specific actions to disable the account of the user that attempts to guess the BS Web Client PIN with brute force attack.
T.MASQUERADE	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. The O.OTP requires that the TOE shall implement a mechanism for authentication based on One Time Password (OTP) which sent the PIN to the BS Web Client user via a predefined e-mail or cell phone number. 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.
T.FILL_RECORDS	An attacker may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity. OE.LOG_STORE requires that the TOE Environment provide a storage system capable of storing at least 120 days of logs.
T.CRASH	A system failure or system crash makes unusable the current installation of the TOE. O.CRASH objective permits to recover the TOE configuration in event to disaster or to restore the TOE previous installation. OE.BACKUP requires that the TOE Environment provide a secure back-up of DBMS and storage data.
T.INTERR	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. OE.CONTINUITY requires that the TOE Environment provides a system to ensure operational continuity in the event of power failure. OE.BACKUP requires that the TOE Environment provide a secure back-up of DBMS and storage data. The OE.STAFF objective ensures competent administrators will manage the TOE.
T. PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. 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.

THREAT, POLICIES, ASSUMPTION	
P.ACCOUNT	Users of the TOE shall be accountable for their activities and operations performed on a given file. The O.IDENTIFY objective supports this objective by ensuring each user is uniquely identified. 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. OE.TIME requires that the TOE Environment provide reliable time reference to be used in the audit logs.
P.PROTECT	The TOE shall be protected from unauthorized access to its functions and data. The O.IDENTIFY objective provide users identification prior to any TOE data access. The O.ACCESS objective only permit authorized users to access TOE functions. The O.CRYPTO objective state that the TOE encrypts the files and logs before storing them, according to the owner's user profile. 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. The OE.STORAGE objective requires the IT Environment to provide the TOE with TOE data storage and retrieval mechanisms. 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. OE.AUDIT _PROTECT requires that the TOE Environment store logs captured and encrypted by the TOE related to management operations performed on the TOE. This prevents threat agents from performing security-relevant actions without detection.
P.MANAGE	The TOE shall only be managed by authorized users. The OE.STAFF objective ensures competent administrators will manage the TOE. 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.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. 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 objective support this policy as those responsible for the TOE must ensure that access to the database via mechanisms outside the TOE boundary is restricted to authorized administrative users only.
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. O.CRASH permits to recover the TOE configuration in event to disaster or to restore the TOE previous installation; OE.CONTINUITY ensures that the operational environment provides a system to ensure business continuity in the event of a power failure; OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE. OE.BACKUP ensures that the operational environment provides a secure back-up of DBMS and Storage data.
P.AUDITLOG	OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE. OE.AUDIT_PROTECT objective ensures that the operational environment provides the capability to protect the integrity of audit log files generated by the TOE via mechanisms outside the TSF. OE.LOG_STORE requires that the TOE Environment provide a storage system capable of storing at least 120 days of logs. OE.TIME requires that the TOE Environment provide reliable time reference to be used in the audit logs.
P.INTEGRITY	The O.INTEGRITY objective ensures the protection of TOE data from modification. The OE.AUDIT_PROTECT objective ensures the integrity of audit records in the database

THREAT, POLICIES, ASSUMPTION	
	generated by the TOE using access mechanisms outside the TSF. 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. OE.STORAGE objective support this policy as those responsible for the TOE must ensure that access to the storage via mechanisms outside the TOE boundary is restricted to authorized administrative users only. O.ACCESS objective supports this policy as the TOE shall allow authorized users to access only to authorized TOE functions and data. The OE.DB objective support this policy as those responsible for the TOE must ensure that access to the database via mechanisms outside the TOE boundary is restricted to authorized administrative users only. O.AUDIT_PROT requires that the TOE capture logs of management operations performed on the TOE. This prevents threat agents from performing security-relevant actions without detection. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses via the web interface. The O.CRYPTO objective state that the TOE encrypts the files and logs before storing them, according to the owner's user profile.
A.TRAINING	OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE.
A.USERS	OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, 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 coordinated with TOE administrator such that only authorized users may utilize the mechanisms.
A.RESTRICT	OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE.
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 coordinated with TOE administrator such that only authorized users may utilize the mechanisms.
A.ALIGNEDBACKUPS	OE.BACKUP ensures that operational environment provides a secure backup of DBMS and storage data.
A.REDKEY	OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE.
A.TRUST	OE.STAFF ensures that personnel working as authorized administrator shall be faithfully selected, skilled and trained for proper operation without compromising the TOE.
A.TIME	A.TIME assumption is upheld by OE.TIME objective requiring the operational environment to provide a reliable time reference.
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.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.BACKUP	OE.BACKUP ensures that operational environment provides a secure backup of DBMS and storage data.
A.SECCOMM	OE.CRYPTO ensures that all communications between TOE components and between the TOE and remote users is protected.
A.INTEGRITY	OE.INTEGRITY ensures that operational environment provides a mechanism that protects the integrity of executable files using .NET framework technology.

Table 14: Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 EXTENDED COMPONENTS DEFINITION

5.1. EXTENDED COMPONENTS DEFINITION

[70] This Security Target does not include any extended components.

6 SECURITY REQUIREMENTS

[71] 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

[72] 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			
FDP – User Data Protection					
FDP_ACC.1	Subset access control	x			
FDP_ACF.1	Security attribute based access control	x			
FDP_ITC.2	Import of user data with 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_ITT.1	Basic internal transfer protection	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		
FPT_RCV.1	Manual recovery	x			
FPT_ITT.1	Internal TOE TSF data transfer		x		
FMT – Security management					
FMT_MTD.1	Management of TSF data	x	x		
FMT_MOF.1	Management of security functions behaviour	x	x		
FMT_MSA.1	Management of security attributes	x	x		
FMT_MSA.3	Static attribute initialization	x	x		
FMT_SMF.1	Specification of Management Functions	x			x
FMT_SMR.1	Security Roles	x			
FCS – Cryptographic support					
FCS_COP.1	Cryptographic operation	x			
FCS_CKM.1	Cryptographic key generation	x			
FPR – Privacy					
FPR_UNO.1	Unobservability	x			

Table 15: List of SFR and related operations

[73] 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

[74] **FAU_GEN SECURITY AUDIT DATA GENERATION**

FAU_GEN.1 Audit data generation

FAU_GEN.1.1
The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the *not specified* level of audit; and
c) *auditable events defined in table 26 and 27 of paragraph* SF_2: Audit

FAU_GEN.1.2
The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *IP address of End User's device*.

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.

[75] **FAU_SAR: SECURITY AUDIT REVIEW**

FAU_SAR.1 (1) Audit review

FAU_SAR.1.1
The TSF shall provide *GAM, authorized GAR and PU* with the capability to read *all audit information in table 26* 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 *SU, GrA* with the capability to read *all audit information in table 27* 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

[76] **FIA_AFL: AUTHENTICATION FAILURE**

FIA_AFL.1 Authentication failure handling/user account lock

FIA_AFL.1.1
The TSF shall detect when *an administrator configurable positive integer within 1 to 100* 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 *lock the user account*.

[77] **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.

[78] **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 (PIN), 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 (PIN) and only if the first authentication step is successfully it is required to enter a OTP that is sent to the user via a predefinited e-mail or cell phone number.*

[79] **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 identity,*
- *User state (active/inactive),*
- *Default Permission Set (a permission set to use to assign the default permissions to objects created by a user),*
- *Groups,*
- *Roles (GAM, GAR, PU, GrA, SU, U, G),*
- *User Privileges (See Table* 16*).*

Privileges	Description (see § 1.6.3 Boole Server users profiles)
Guest	User has Guest privileges
User	User has User privileges
GrA	User has Group Administrator privileges
SU	User has Super User privileges
PU	User has Power User privileges
GAR	User has General Administrator restricted privileges
GAM	User has General Administrator Master privileges

Table 16: User Privileges

[80] **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 meet

- *at least eight characters;*
- *at least one number;*
- *and at least one uppercase letter*.

6.1.3. USER DATA PROTECTION

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

FDP_ACC.1 Subset access control

FDP_ACC.1.1
The TSF shall enforce the *Boole Server access control SFP* on *Subjects: User; Objects: BS Server, BS Web Client; Operations among subjects and objects covered by the SFP: login to BS Server and login to BS Web Client.*

[82] **FDP_ACF ACCESS CONTROL FUNCTIONS**

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1
The TSF shall enforce the *Boole Server 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:* **Security Attribute based access control***.*

Subjects	**Security Attribute of Subjects**	**Objects**	**Security Attribute of Objects**	***Rules governing access among controlled subjects and controlled objects***
User	Username, password.	BS Server	User Privileges.	The user shall access to BS Server panel providing a valid Username and password. User privileges define the operations that a user can perform on BS Server via BS Server panel.
User	Username, PIN, Group.	BS Web Client	User Privileges.	The user shall access to BS Web Client providing a valid Username, PIN and Group. User privileges define the operations that a user can perform on BS Server via BS Web Client panel.
User	Current Access attempts.	BS Web Client	Number of Max Access attempts allowed.	The user shall provide a valid PIN within a settable number of max access attempts.
User	One Time Password.	BS Web Client	One Time Password flag set.	If Strong Authentication is enabled, user also shall provide a valid One Time Password to access to BS Web Client.
User	User IP address.	BS Web Client	User IP address allowed.	If IP restriction is enabled, the user can connect to BS Web Client only using an authorized IP address.

Table 17: Security Attribute based access control

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: *none*.

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

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

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1
The TSF shall enforce the *Boole Server flow control SFP* on

Subjects: *BS Server, DBMS, BS Agent, Storage.*

Information: *Passphrase, Audit Log, Owned file, Encrypted Owned file.*

Operations: *Passphrase Upload (from BS Server to DBMS), Audit Log Upload (from BS Server to DBMS), Owned file Upload (from BS Agent to Storage), Owned File Download (from Storage to BS Agent).*

FDP_IFF.1 Simple security attributes

FDP_IFF.1.1
The TSF shall enforce the *Boole Server 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 below:*

Subjects	**Subject security attributes**		**Possible values**
BS Server	-		-
	-		-
BS Agent	-		-
Storage	-		-
DBMS	-		-
Information	**Information security attributes**		**Possible values**
Passphrase	data state		encrypted / unencrypted
Audit Log	data state		encrypted / unencrypted
Owned file	data state		encrypted / unencrypted
Encrypted Owned file	Id_file_DBMS (Unique identifier of the file in the Database)		null / not null
	Id_file_Storage (Unique identifier of the file in the Storage)		null / not null
	DBMS record	Owner ID	correct / incorrect
		CRC	
		File size	

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 below:*

Operation	**Security Attribute-based relationship between subject security attributes and information security attributes**
Passphrase or Audit Log Upload (from BS Server to DBMS)	The operation takes places if: - State of passphrase or audit log = encrypted
Owned File Upload (from BS Agent to Storage)	The operation takes places if: - State of Owned file = encrypted
Owned file Download (from Storage to BS Agent)	The operation takes places if: - Owner Id = correct - Encrypted Owned file CRC = correct - File size = correct - Id_file_DBMS = not null - Id_file_Storage = not null

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*.

[84] **FDP_ITC: IMPORT FROM OUTSIDE OF THE TOE**

FDP_ITC.2 Import of user data with security attributes

FDP_ITC.2.1
The TSF shall enforce the *Boole Server 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: *none*

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

FDP_ETC.2 Export of user data with security attributes

FDP_ETC.2.1
The TSF shall enforce the *Boole Server 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: *none*.

[86] **FDP_ITT: INTERNAL TOE TRANSFER**

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1
The TSF shall enforce the *Boole Server flow control SFP, Boole Server access control SFP* to prevent the *disclosure*, *modification* of user data when it is transmitted between physically-separated parts of the TOE.

6.1.4. PROTECTION OF THE TSF

[87] **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 *CRC of the encrypted owned file* when shared between the TSF and another trusted IT product.

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

Note_1: *Note: The rules "Encrypted file check" is referred to § "7.1.3 SF_3: Encryption"*

[88] **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 18*.

FPT_TEE.1.2 If the test fails, the TSF shall *show error message and blocks the installation*.

External entity	List of properties
Web Server	Presence of software prerequisites as specified in §1.5.3.1
Storage system	Presence of connectivity, path of storage system
DBMS	Presence of connectivity, required DBMS type
End user PC	Presence of software prerequisites as specified in §1.5.3.2

Table 18: list of properties of the external entities

[89] **TRUSTED RECOVERY (FPT_RCV)**

FPT_RCV.1 Manual recovery

FPT_RCV.1.1 After *a TOE crash* the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.

[90] **INTERNAL TOE TSF DATA TRANSFER (FPT_ITT)**

FPT_ITT.1 Basic internal TSF data transfer protection

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

6.1.5. SECURITY MANAGEMENT

[91] **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 19* the *TSF data specified in Table 19* to *authorized identified roles specified in Table 19.*

Authorized roles	TSF Data	Operation Allowed
GAM	REDKEY	Create, modify
	GAR user profile	Create, modify, delete
	SU user profile	Create, modify, delete
	BS Server Log file (event and malfunctions)	View, delete

Authorized roles	TSF Data	Operation Allowed
	Log of General Administrator Master Log of General Administrator Restricted Log of Power User	View
	Number of operation that GAR is allowed to perform	Set, modify
	BS Server parameters	set, modify, restore
	User password	Create_default, modify, delete.
authorized GAR	BS Server setup parameters	modify
	SU user profile	Create, modify, delete
	Group’s profile	Create, modify, delete
	User profile (within created groups)	Create, modify, delete, block, unblock, clone, add alias, modify alias, remove alias.
	User profile (within different groups)	Move from a group to another, remove, add alias, modify alias, remove alias.
	User password	Create_default, modify, delete.
	Centralized space	Assign
	log of General Administrator Restricted log of Power User	View
PU	Group structure log of General Administrator Master log of General Administrator Restricted log of Power User	view
SU	Group	Create, assign a group administrator GrA
	GrA user profile	Create, modify, delete, unlock.
	GrA user PIN	Create_default, modify, delete.
	User profile (within created groups)	Create, modify, delete, unlock, clone,
	User profile (within different groups)	Move, remove, block, unblock.
	User PIN (within created groups)	Create_default, modify, delete
	Advanced Identity Platform parameters	Change
	log of Super User log of Group administrator log of User log of Guest	View (from Web-client panel)
GrA	User profile (within his group)	Create_default, modify, delete, block, unblock, view the activities performed by
	User PIN (within his groups)	Create, modify, delete
	Centralized space	Assign
	log of Group administrator log of User log of Guest	View (from Web-client panel)
User	PIN	Change_default.
Guest		
	PIN	Change_default.

Table 19: Management of TSF data

[92] Note: The **BS Server parameters** are the following

General Administrator parameters:

- Administrator profile
- Administrator log
- REDKEY
- number of operations authorized

Boole Server Groups parameters:

- Boole Server Profiles
- Synchronization delay between BS Sever and Active Directory server
- Active Directory query type
- Boole Server Group name
- space assigned to a Boole Server Group
- Administrator profile of a Boole Server Group
- Removing a Boole Server Group
- User profile
- Guest profile
- Super Users profile
- Active Directory synchronization time
- Advanced group settings (maximum number of generable profiles, set up groups visibility option)
- File signature

Server Setup parameters:

- IP address and port of Boole Server that BS Web Client must be connected
- IP address of the machine on which you install the Boole Server Web Client

Storage parameters:

- Path of archive unit
- Path and command-line parameters of application used for storage backup

Database parameters:

- Database type, name and address
- Cache of database connections (connection pool)
- Username and password

SMTP server parameters:

- SMTP address and port of the outgoing mail server
- SMTP username and password (If the SMTP server requires a secure connection)
- SMS gateway and SSL connection options

Boole Server Farm parameters:

- IP address and port of primary server
- IP address and port of fail-over/load-balance server

Remote Drive parameters:

- Username authorized to access the network driver from a remote connection;
- Path of network driver

Options parameters:

- Users Log period (days)
- System log on/off option
- Boole Server “check for update” option
- BS Agent automatic update option
- Watermark settings
- Password complexity settings
- End user client session timeout (minutes).

[93] Note: The Advanced Identity Platform parameters can be set by the BS Web Client Panel and by BS Server Panel:

Advanced Identity Platform parameters – BS Web Client Panel:

- Profile options
- Access rules
- Agent options
- Platform options
- Top Secret options

Advanced Identity Platform parameters – BS Server Panel:

- Profile options
- Access rules
- Agent options
- Platform options
- Top Secret options
- Certified applications options
- User timetables rules
- File protection rules
- Mail Encryptor options

[94] **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 to *determine the behavior of, disable, enable, modify the behavior of* the functions *as specified in table 20* to *roles as identified in table 20*.

Authorized roles	Ability to	Functions
GAM	determine the behavior of	TOE Installation TOE recovery TOE restore
	determine the behavior of	Server Setup function – BS Server Panel
	determine the behavior of	General Administration function – BS Server Panel
	determine the behavior of	Boole Server Groups function – BS Server Panel
	determine the behavior of	Advanced Identity Platform function – BS Server Panel
	determine the behavior of	Storage Function – BS Server Panel
	determine the behavior of	Options function – BS Server Panel

Authorized roles	Ability to	Functions
GAM, authorized GAR	modify the behavior of	Server Setup function – BS Server Panel
	modify the behavior of	General Administration function – BS Server Panel
	modify the behavior of	Boole Server Groups function – BS Server Panel
	modify the behavior of	Advanced Identity Platform function – BS Server Panel
	modify the behavior of	Storage Function – BS Server Panel
	modify the behavior of	Options function – BS Server Panel
SU	determine the behavior of	Profile Manager functions – Web Client Panel
	determine the behavior of	Auditing functions – Web Client Panel
	determine the behavior of	Advanced Identity Platform function – Web Client Panel
GrA	modify the behavior of	File Manager functions – Web Client Panel
	modify the behavior of	Profile Manager functions – Web Client Panel
	modify the behavior of	Auditing functions – Web Client Panel
	modify the behavior of	Secure Messenger functions – Web Client Panel
	modify the behavior of	Advanced Identity Platform function – Web Client Panel
U	modify the behavior of	File Manager functions – Web Client Panel
	modify the behavior of	Secure Messenger functions – Web Client Panel
PU, G	none	none

Table 20: Management of security functions

[95] **<u>FMT_MSA: MANAGEMENT OF SECURITY ATTRIBUTES</u>**

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1
The TSF shall enforce the *Boole Server access control SFP* to restrict the ability to *<u>change_default, query, modify, delete</u>*, *create* the security attributes *defined in Table 21* to the *authorized identified roles specified in Table 21*.

Authorized role	Ability to	Security Attribute
GAM	create change_default, query, modify, overwrite	Username, Password , Group, User Privilege Redkey
	delete	Username Password Group User Privilege

	create,
	change_default,
	query,
	modify
		One Time Password flag;
		User IP address allowed;
		Number of Max Access attempts allowed.

GAR	change_default, query, modify, delete.	Username, Password, Group, User Privileges.

	change_default,
	query,
	modify
		One Time Password flag;
		User IP address allowed;
		Number of Max Access attempts allowed.

	Query.	Current Access attempts.

PU	query	One Time Password flag;
		User IP address allowed;
		Number of Max Access attempts allowed;
		Current Access attempts.

SU	create, query, modify	Username, PIN, Group, User Privileges.
GrA	query, modify	Username, PIN, Group, User Privileges.
U	none	none
G	none	none

Table 21: Management of security attributes

FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1
The TSF shall enforce the *Boole Server access control SFP* to provide <u>*permissive*</u> default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2
The TSF shall allow the GAM, GAR *and GrA* to specify alternative initial values to override the default values when an object or information is created.

[96] FMT_SMF SPECIFICATION OF MANAGEMENT FUNCTIONS

FMT_SMF.1 (1) Specification of Management Functions

FMT_SMF.1.1 – Management via BS Server panel

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

- *General Administration*
- *Groups Administration*
- *Advanced Identity Platform*
- *Storage*
- *Server Setup*
- *Option*

FMT_SMF.1 (2) Specification of Management Functions

FMT_SMF.1.1 - Management via BS Web Client panel

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

- *File Manager*
- *Profile Manager*
- *Advanced Identity Platform*
- *Audit*
- *Secure Messenger*

[97] FMT_SMR: SECURITY MANAGEMENT ROLES

FMT_SMR.1 Security roles

FMT_SMR.1.1

The TSF shall maintain the roles *GAM, GAR, GrA, PU, SU, U, G*.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.1.6. CRYPTOGRAPHIC SUPPORT

[98] **FCS_COP: CRYPTOGRAPHIC OPERATION**

FCS_COP.1 Cryptographic operation

FCS_COP.1.1
The TSF shall perform owned file *encryption and decryption, passphrases encryption and decryption, red key encryption and decryption, audit log encryption and decryption* in accordance with a specified cryptographic algorithm *RC6-32/20*[1] and cryptographic key sizes 255 bytes (*2040 bit)* that meet the following: *RC6 algorithm standard [RC6]*.

[99] **FCS_CKM: CRYPTOGRAPHIC KEY MANAGEMENT**

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1
The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Boole Server proprietary algorithm* and specified cryptographic key sizes *255 byte* that meet the following: *none*.

[100] **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 *BS Agent users*.

[1] Any reference to RC6 Algorithm is to be considered as a reference to RC6-32/20

6.2. SECURITY ASSURANCE REQUIREMENTS

[101] 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.

[102] 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*.

[103] 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 22: Security Assurance Requirements

6.3. SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

6.3.1. CC Component Dependencies

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

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

SFR	DIPENDENCY	RATIONALE
FAU_GEN.1	FPT_STM.1	Satisfied by OE.TIME in the environment
FAU_GEN.2	FAU_GEN.1	Satisfied
	FIA_UID.1	Satisfied by FIA_UID.2, hierarchical to FIA_UID.1
FAU_SAR.1	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
FIA_UID.2	-	-
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2, hierarchical to FIA_UID.1
FIA_UAU.5	-	-
FIA_ATD.1	-	-
FIA_SOS.1	-	-
FDP_ACC.1	FDP_ACF.1	Satisfied
FDP_ACF.1	FDP_ACC.1	Satisfied
	FMT_MSA.3	Satisfied
FDP_ITC.2	FDP_IFC.1	Satisfied
	FPT_TDC.1	Satisfied
	FTP_TRP.1	This requirement is not relevant to countering threats and for fulfill the objectives of security because the userdata exchanged between BS Server and Storage is transmitted encrypted.
FDP_ETC.2	FDP_IFC.1	Satisfied
FDP_IFF.1	FDP_IFC.1	Satisfied
	FMT_MSA.3	This requirement is not applicable for Boole Server flow control SFP because the security attributes specified into Boole Server flow control SFP are not manageble by any user role.
FDP_IFC.1	FDP_IFF.1	Satisfied
FDP_ITT.1	FDP_ACC.1	Satisfied
	FDP_IFC.1	Satisfied
FPT_TDC.1	-	-
FPT_TEE.1	-	-
FPT_RCV.1	AGD_OPE.1	Satisfied
FPT_ITT.1	-	-

FMT_MTD.1	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_MOF.1	FMT_SMR.1	Satisfied
	FMT_SMF.1	Satisfied
FMT_MSA.1	FMT_SMF.1	Satisfied
	FMT_SMR.1	Satisfied
	FDP_ACC.1	Satisfied
FMT_MSA.3	FMT_MSA.1	Satisfied
	FMT_SMR.1	Satisfied
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1	Satisfied by FIA_UID.2, hierarchical to FIA_UID.1
FCS_COP.1	FCS_CKM.4	The requirement is not applicable because RC6 cryptographic keys are never stored in the hard disk. Also the passphrases from which are generated the encryption keys are never deleted but, depending on the case, kept in protected mode into the database or in the operating system or released by the operating system after their use since they are not stored in the hard disk but only kept in RAM.
	FCS_CKM.1	Satisfied
FCS_CKM.1	FCS_COP.1	Satisfied
	FCS_CKM.4	The requirement is not applicable because RC6 cryptographic keys are never stored in the hard disk. Also the passphrases from which are generated the encryption keys are never deleted but, depending on the case, kept in protected mode into the database or in the operating system or released by the operating system after their use since they are not stored in the hard disk but only kept in RAM.
FPR_UNO.1	-	-

Table 23: 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.ACCESS	O.MANAGE	O.IDENTIFY	O.CONFIDENTIAL	O.CRYPTO	O.INTEGRITY	O.CRASH	O.ANTI_BRUTE	O.STRONG_KEYS	O.CONFIG	O.OTP
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
FIA_ATD.1					X								
FIA_SOS.1			X		X								
FDP_ACC.1			X										
FDP_ACF.1			X										
FDP_ITC.2							X						
FDP_ETC.2							X						
FDP_IFC.1		X					X						
FDP_IFF.1		X					X						
FDP_ITT.1								X					
FMT_MTD.1			X	X				X					
FMT_MOF.1				X									
FMT_MSA.1			X										
FMT_MSA.3			X										
FMT_SMF.1			X	X									
FMT_SMR.1				X									
FCS_COP.1							X				X		
FCS_CKM.1											X		
FPT_TDC.1								X					
FPT_TEE.1												X	
FPT_RCV.1									X				
FPT_ITT.1		X						X					

SFR/O	O.AUDIT	O.AUDIT_PROT	O.ACCESS	O.MANAGE	O.IDENTIFY	O.CONFIDENTIAL	O.CRYPTO	O.INTEGRITY	O.CRASH	O.ANTI_BRUTE	O.STRONG_KEYS	O.CONFIG	O.OTP
FPR_UNO.1						X							

Table 24: Mapping of TOE SFRs to Security Objectives

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

OBJECTIVE	RATIONALE
O.AUDIT	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]. The TOE provides GAM, GAR, PU, SU and GrA 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].
O.AUDIT_PROT	The TOE protects audit information generated by itself from disclosure and modification when transmitted between BS Web Client and BS Server or between BS Agent and BS Server [FPT_ITT.1]. [FDP_IFC.1] and [FDP_IFF.1] establish Boole Server flow control security policy which lay down the rules that the TOE must follow to ensure that the exchange of audit log between the TOE and DBMS takes place only if the audit log is encrypted.
O.ACCESS	Users authorized to access the TOE are determined using an identification and authentication process [FIA_UAU.2, FIA_UID.2] [FDP_ACC.1] [FDP_ACF.1]. The permitted access to TOE data by the roles and permissions is defined [FMT_MTD.1, FMT_SMF.1]. The TOE specifies metrics for password complexity in authentication [FIA_SOS.1]. The management of security attributes is restricted [FMT_MSA.1.] The default values of security attributes are restrictive in nature [FMT_MSA.3].
O.MANAGE	Specification of Management functions requires that the TSF provide specific management functions [FMT_SMF.1]. Management of TSF data allows authorized users to manage TSF data [FMT_MTD.1]. 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]. Security roles specifies the roles with respect to security that the TSF recognizes [FMT_SMR.1].
O.IDENTIFY	Security attributes of subjects used to enforce the security policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are determined using a identification process upon username/password combination [FIA_UID.2 and FIA_UAU.2]. The TOE specifies metrics for password complexity in authentication [FIA_SOS.1].

OBJECTIVE	RATIONALE
O.CRYPTO	TOE requires a cryptographic operation to be performed in accordance with a RC6 algorithm and with a cryptographic key of 2040 bit. [FCS_COP.1] [FDP_IFC.1] and [FDP_IFF.1] establish Boole Server 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 is encrypted. [FDP_ITC.2] and [FDP_ETC.2] enforce the Boole Server flow control security policy ensuring that security attributes correctly represent the user data and are accurately and unambiguously associated with the user data imported end exported from Storage systems.
O.INTEGRITY	The TOE protects all TSF data from modification when are transmitted between BS Web Client and BS Server or between BS Agent and BS Server [FPT_ITT.1]. The TOE implements Encrypted file check rule when interpreting the TSF data from DBMS [FPT_TDC.1]. The TOE implements a control access security policy and a flow control security policy to prevent disclosure and modification of user data when it is transmitted between BS Agent e BS Server [FDP_ITT.1]. Only authorized administrators of the System may query or add TOE data [FMT_MTD.1].
O.ANTI_BRUTE	The TOE requires that the TSF shall be able to terminate the session establishment process after a specified number of unsuccessful user authentication attempts (within 1 to 100 configurable by the GAM/GAR). It also requires that, after termination of the session establishment process, the TSF shall be able to lock the user account from which the attempts were made when the defined number of unsuccessful authentication attempts has been *surpassed*. [FIA_AFL.1]
O.STRONG_KEYS	The TOE requires a cryptographic operation to be performed in accordance with a RC6 algorithm and with a cryptographic key of 2040 bit. [FCS_COP.1] The TOE ensures the generation of cryptographic keys with a length of 255 bytes (2040 bits) in accordance with a proprietary cryptographic key generation algorithm. [FCS_CKM.1]
O.CONFIDENTIAL	With “Anti photo” option activated the TOE ensure that unauthorized user are unable to observe the entire screen of the BS Agent user while consult his file. [FPR_UNO.1]
O.CONFIG	The TOE during installation process performs tests on external entities in order to ensure compliance with the pre-required software. [FPT_TEE.1]
O.CRASH	The TOE ensure that after a TOE crash it’s possible to return to a secure state via a manual recovery [FPT_RCV.1].
O.OTP	The TOE implements a multiple authentication mechanism based on static password (PIN) and One Time Password that is sent to the user via predefinited e-mail or cell phone number [FIA_UAU.5].

Table 25: Rationale for TOE Security Objectives coverage by SFRs

7 TOE SUMMARY SPECIFICATION

7.1. SECURITY FUNCTION

[107] 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 = Audit
SF_3 = Encryption
SF_4 = Management
SF_5 = Centralized Access Control

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

7.1.1. SF_1: Identification and Authentication

[109] The TOE users GAM, GAR and PU must login with a valid Username and Password supplied via BS Server panel while the TOE users SU, GrA, U and G must login with Username, PIN and Group supplied via Web Client panel.

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

[111] In case of incorrect login on BS Web Client by a user the Web Client login is repeated, but after a defined number of failed login attempts, the user is blocked.

[112] In case of incorrect login on BS Server by an administrative user the login panel is repeated after a certain period of time that increases with every failed login attempt.

7.1.1.1. Functions of identification and authentication

[113] The following functions are available to GAM, GAR via BS Server Panel and are available to SU and GrA via BS Web Client panel.

[114] **Force PIN change**: by flagging this option, at first access the BS Web Client user will be asked to change the PIN he has been assigned. The PIN must have at least the following minimum security requirements:

- at least eight characters;
- at least one number;
- and at least one uppercase letter.

[115] **Allow New PIN request:** by enabling the “Allow new PIN request” option, it is possible to allow BS Web Client users to request a new PIN in case the old one has been forgotten. All the users who require it, will receive via e-mail a new PIN valid for a single use, which will allow them to access the system and change the temporary PIN with a new one.

[116] The following functions are available only to SU and GrA, U and G via BS Web Client panel.

[117] **Strong Authentication:** by flagging the “Enable Strong Authentication” option, it is possible to activate the Strong Authentication mode during login. With Strong Authentication, BS Web Client users, after having entered their ID access credentials (Username, PIN and Group), need to enter in the following window a One Time Password, which can be requested through the relevant link and sent to users via e-mail or by SMS.

[118] **Maximum number of access attempts:** by enabling the “Maximum number of access attempts”, it is possible to set the maximum number of failed authentication attempts allowed before a profile, will be temporarily blocked.

[119] **IP restriction**: by enabling the “IP restriction” option, Boole Server allows to associate a list of IP addresses to each profile from where the access is authorized. The profile that activates the IP restriction will be able to connect to Boole Server only using one of the IP addresses specified by the side server administrator. Thanks to this functionality, the IP is meant to be one of the main identifier through which the access is authorized.

7.1.2. SF_2: Audit

[120] Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities, i.e. each actions 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.

[121] Each action logged, including the start-up/shut-down of the security audit function, includes the date and time of the event, the ID of the user that caused the action, and indication whether the event is a failed action, for example a failure to authenticate.

[122] **Auditing of GAM/GAR log:** Through the control panel provided by BS Server, the GAM can see the log of the operations perform by administrative users. GAR and PU also can see the log according to the permissions granted by GAM. This is only possible by inserting the REDKEY . The categories of auditable operations are listed in table 26. It is also possible filter the events by defining a time range which by default is set to 1 day.

Administrative Profile – Auditable events categories
Login
General Administrator
Boole Server Groups
Storage
Server setup
Advanced Identity Platform
Options
License
Service

Table 26: Auditable Events for Administrative profile

[123] **Logging all operations performed by client**: Through the control panel provided by BS Server, it's possible enable or disable the log of all operations performed by the users accessing via BS Web Client. Operations that are recorded are listed in table 27 TOE logs also the IP address of the end users that accesses the Web client.

File - auditable events
Folder upload/creation
Download
File sharing
File/folder renaming
File/folder moving
File/folder deletion

File/folder restoring
File editing
File viewing
File copying
Restore data
Encrypt (Remote Drive)
Extract (Remote Drive)

Table 27: Auditable Events performed by Web Client users

[124] **Enabling Auditing:** Through the control panel provided by BS Server the administrative users can enable the Auditing section of the BS Web Client . In this way the group administrator (GrA) and the super user (SU) can view the operations performed by the Web Client Users.

[125] The Boole Server accounting services allow the GAM/GAR profile:

- to set Users log period (Log file of all operations performed by any Boole Server end users is stored encrypted in the database for a default period of 120 days);
- to enable or disable the System log option: log file of all security events and malfunctions processed by the BS Server.

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

7.1.3. SF_3: Encryption

[127] Encryption security function implements RC6 symmetric algorithm with 2040 bit key length (255-byte key). RC6 is proprietary algorithm, patented by RSA Security and it’s used by default.

[128] All user data are encrypted and stored in the storage system. To ensure the confidentiality of information protected by Boole Server, the decryption keys are stored centrally in the DBMS and not together with the file itself. The encryption/decryption keys are derived from passphrases that change for each file.

[129] **Secure Channel: Encryption process**

[130] The encryption process is applied between the two extremes of the communication channel with the purpose of securing the channel. The two ends of the channel (End User and Server) depend on the configuration in which the TOE is working (see § 1.5.1).

[131] In configuration 1 the secure channel is established between the BS Web Client component and the BS Server component.

[132] In configuration 2 the secure channel is established between BS Agent component and BS Server component.

[133] The operational environment is configured to establish always, regardless of the configuration of the TOE, an HTTPS channel based on AES 256 between End user and Server.

[134] The operational environment supports the TOE functions by implementing random number generation and RSA 512-bit encryption during the initial handshake upon setting up the secure channel between BS Server and BS Web Client (if TOE in configuration 1) or between BS Server and BS Agent (if TOE in configuration 2).

[135] The RC6 cryptographic keys used to implement a secure channel between separate parts of the TOE change for each connection.

[136] **Cryptographic key generation**

The generation of a specific RC6 255 bytes encryption key is obtained by a proprietary algorithm of Boole Server from a passphrase which has different length and different generation modes that may or may not involve the TOE environment (for example when the passphrase is based on .NET CNG Cryptography API Next Generation) depending on the operation for which encryption is used.

Details on Boole Server RC6 cryptographic key generation algorithm have been provided in TOE Design documentation.

[137] **DBMS Data encryption**

Passphrase, Audit log and reference to files are protected when stored in the DBMS through RC6 symmetric encryption using the REDKEY as a passphrase.

[138] **Encrypted file check**

When a encrypted owned file needs to be read from the Storage, the CRC of 32 bytes central of encrypted file is calculated and then compared with the same CRC previously calculated and stored in the DB. The CRC is used to detect any random changes that occurred during the permanence of the file on the storage system. If this comparison fails BS Server retrieve an error message and it denies the data retrieval; otherwise the required user data are transferred from Storage to BS Server.

7.1.4. SF_4: Management

[139] Boole Server’s Granular and Dynamic Rights Management, allows real time editing of any users 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”. The TOE’s management security function provides administrator support functionality to configure and manage TOE.

[140] Management of the TOE may be performed via BS Server panel or Web Client Panel.

[141] **MANAGEMENT OF THE TOE VIA BS SERVER PANEL**
Below are the functions that the BS Server component allows you to manage through its panel:

- **General administration function – BS Server Panel**
  The General Administrator section lets edit properties of profiles that have access to the Boole Server control panel.
- **Boole Server Groups administration function – BS Server Panel**
  The Boole Server Group function lets to set and edit the properties of Boole Server Groups.
- **Advanced Identity Platform function (AIP) – BS Server Panel**
  The A.I.P. Advanced Identity Platform functions allows GAM/GAR to configure several enhanced security parameters, in order to make it even more strict and secure for users to access information.
- **Storage Function – BS Server Panel**
  The Storage function lets GAM/GAR to manage data storage units and mirror units which have been configured for the TOE.
- **Server Setup function – BS Server Panel**
  The Server setup function lets GAM/GAR to change the settings to a server on which Boole Server has been installed and allows GAM/GAR to activate several security systems to protect the network managed by Boole Server and configure a Boole farm in order to run Failover and Load Balance systems.
- **Options function – BS Server Panel**

The Options functions lets GAM/GAR to change many Boole Server settings and access functions such as Log file and Watermark.

[142] **MANAGEMENT OF THE TOE VIA BS WEB CLIENT PANEL**

[143] The web client TOE management is done via a browser-based management console, protected by an SSL session provided by the operational environment. Management permission are defined per-group and per-user.
Below are the functions that the BS Web Client component allows to manage through its panel:

- **File Manager functions**
  These functions allows to manage all operations related to file centralization, management and sharing.
- **Profile Manager functions**
  These functions allows to manage all operations related to the configuration and management of the profiles belonging to the connected Group (only authorized Administrator or Super User profiles can access this area). Only Administrators and Super Users can be authorized to modify a profile belonging to their group.
- **Auditing functions**
  These functions to view the tracking of the operations performed by the users belonging to the connected Group (only authorized Administrator or Super User profiles can access this area).
  It is possible manage Auditing functionality only if you have an authorized Administrator or a Super User profile. In this case It is possible to view all the operations performed on files belonging to your own resources.
- **Secure Messenger functions**
  These functions allows to encrypt or decrypt texts and e-mail messages.

7.1.5. SF_5 Centralized Access Control

[144] With Centralized Access Control security functions only authorized users can work directly on the protected files, being able to share them with other users according to highly controlled policies.

[145] 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.

[146] Secured files can be transferred via the Client or emailed to the recipient as an attachment. Once delivered, the correct file access policy is applied according to the latest version; ensuring appropriate access is always maintained.

[147] Boole Server users have the ability to access protected information from anywhere and at anytime 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 Boole Server for each operation required.
Boole Server provides a framework to define the appropriate access rights to a file.

[148] **FILE SHARING PROTECTION**
Boole Server Web Client offers a number of options related to the different types of protection you can apply on files:

- **SIMPLE SHARING**: to share the selected resources in decryption mode, without any ciphering protection;

- **ENCRYPTED SHARING**: to share the selected resources in encryption mode.

Protection level to apply to the selected file:

- Read-only: High level functional limitation - Red led: Users are authorized to view the file, but cannot edit it.
- Restricted: Medium level functional limitation - Yellow led: Users are authorized to open, edit and update files, but cannot copy them.
- Unlimited: Low level functional limitation - Green led: Users are authorized to perform any operation on files.

- **SHARING IN STREAMING**: to share the selected resources in protected streaming, i.e. a special protected format which is not editable.

- **ANTI PHOTO PROTECTION**: With this option GrA or U can make BS Agent user to display only a portion at a time of shared file to prevent that an unauthorized user can capture the entire user data displayed on the screen.

[149] **SECURE MESSENGER**
Boole Server Web Client allows to send encrypted message via e-mail to Boole Server profiles.
The Limitations screen appears: here it is possible to set limitations associated to the encrypted message that is being configured.

[150] Since you have attached a file to the encrypted message, you need to set the protection level you wish to apply to the selected file by using the vertical cursor:

- Read-only - High level functional limitation - Red led: Users are authorized to view the file, but cannot edit it.
- Restricted - Medium level functional limitation - Yellow led: Users are authorized to open, edit and update files, but cannot copy them.
- Unlimited - Low level functional limitation - Green led: Users are authorized to perform any operation on files.

7.2. TOE SUMMARY SPECIFICATION RATIONALE

[151] 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: I&A	SF_2: Audit	SF_3: Encryption	SF_4: Management	SF_5: Centralized Access Control
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				
FIA_UAU.2	x				
FIA_UAU.5	x				
FIA_ATD.1	x				
FIA_SOS.1	x				
FDP_ACC.1					x
FDP_ACF.1					x
FDP_IFC.1			x		
FDP_IFF.1			x		
FDP_ITC.2			x		
FDP_ETC.2			x		
FDP_ITT.1			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	

	SF_1: I&A	SF_2: Audit	SF_3: Encryption	SF_4: Management	SF_5: Centralized Access Control
FCS_COP.1			x		
FCS_CKM.1			x		
FPT_TDC.1			x		
FPT_TEE.1				x	
FPT_RCV.1				x	
FPT_ITT.1			x		
FPR_UNO.1					x

Table 28: TOE Security Functions/SFRs mapping

[152] 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	**AUDIT** - The TOE generates the log of the operations performed by GAM and GAR from the BS server panel according to the events categories specified in the table 26. The TOE generates the log of the operations performed by all users who access the BS web client panel according to the events categories specified in the table 27. TOE logs also the IP address of the end users that accesses the Web client.
FAU_GEN.2	**AUDIT** - The TOE associates the identity of the user that caused the event for each event logged.
FAU_SAR.1 FAU_SAR.2 FAU_SAR.3	**AUDIT** - Through the control panel provided by BS Server, the GAM can see the log of the operations perform by administrative users. GAR and PU also can see the log according to the permissions granted by GAM. Through the control panel provided by BS Web Client the SU and GrA can see the log of the operations performer by all web client users.
FIA_AFL.1	**Identification and Authentication** – The TOE permits to GAM or GAR to set the maximum number of failed authentication attempts allowed before a profile will be locked.
FIA_UID.2 FIA_UAU.2 FIA_UAU.5	**Identification and Authentication** – The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data. No action can be initiated before proper identification and authentication. If strong authentication is enable, user also shall provide a valid One Time Password to access to BS Web Client.
FIA_ATD.1	**Identification and Authentication –** The TSF maintain a set of security attributes that is used to enforce all the TSFs.
FIA_SOS.1	**Identification and Authentication** – The TSF provides a mechanism to verify that Redkey, BS Server password and BS Web Client PIN meet at least eight characters, at least one number and at least one uppercase letter.

SFR	SF and rationale
FDP_ACC.1 FDP_ACF.1	**Centralized Access Control** – The users shall access to BS Server panel providing a valid username and password. The users shall access to BS Web Client providing a valid Username, PIN and Group. The users shall provide a valid PIN within a settable number of max access attempts. If strong authentication is enable, user also shall provide a valid One Time Password to access to BS Web Client. If IP restriction is enabled the user can connect to BS Web Client only by using an authorized IP address.
FPR_UNO.1	**Centralized Access Control** – GrA and U roles can centrally manage and control access to file shared with external users equipped with BS Agent and can enable an option called Anti Photo Protection. This option can make external users to display only a portion at a time of shared files to prevent an unauthorized user can capture the entire user data displayed on the screen.
FMT_MTD.1 FMT_MOF.1	**Management** – The Administrator status and user permissions determine the access privileges of the user to TOE data and the ability to use TOE security functions.
FMT_MSA.1	**Management** – The TOE ensures the access to the security attributes are restricted as to enforce the access control policy for the TOE.
FMT_MSA.3	**Management** – The TOE ensures the default values of security attributes are restrictive in nature as to enforce the access control policy for the TOE.
FMT_SMF.1	**Management** – The management functions that must be provided for effective management of the TOE are defined and described.
FMT_SMR.1	**Management** – The TOE provides the roles specified in the SFR. When a User Account is created or modified, the role is specified by setting or clearing the Administrator status for the user.
FPT_TEE.1	**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.
FPT_RCV.1	**Management** – The TOE provides a manual recovery mechanism to return to a secure state in case of TOE crash or in the case where it is necessary to restore the initial configuration.
FCS_COP.1 FCS_CKM.1	**Encryption** – Encryption security function implements RC6 symmetric algorithm with 2040 bit key length. The TOE generate cryptographic keys with a length of 255 bytes (2040 bits) in accordance with a proprietary cryptographic key generation algorithm.
FPT_ITT.1	**Encryption** – The TOE provides a secure channel between BS Web Client and BS Server or between BS Agent and BS Server to protect disclosure and modification of TSF data.
FDP_ETC.2 FDP_IFF.1 FDP_IFC.1 FDP_ITT.1	**Encryption –** The TOE performs encryption of all user files, log files and passphrases. The user files are sent to the storage system while the log files and passphrases are sent to the DBMS according to a specific set of rules that guarantee the correct encryption and subsequent interpretation. The TOE protects the TSF data from disclosure and modification when it is transmitted between physically separate parts of the TOE.
FDP_ITC.2 FPT_TDC.1	**Encryption –** When the user file is imported from the storage system the TOE ensures the correct interpretation of it's CRC which is used by the TOE to detect any random changes occurred during the permanence of the files on the storage system.

Table 29: SFR to TSF rationale