



Security Target  
for  
**HOB RD VPN**  
blue edition

Document version:  
2.2

Product version:  
2.1 10.5397

Issue:  
January 15, 2014



HOB GmbH & Co. KG  
Schwadmuehlstrasse 3  
90556 Cadolzburg  
Germany

Ph. +49-9103-715-0  
Fax +49-9103-715-271  
E-mail: [support@hob.de](mailto:support@hob.de)  
Internet: <http://www.hobsoft.com>



# Table of Contents

<a href="#">Symbols and Conventions.....</a>	<a href="#">4</a>
<a href="#">Document history.....</a>	<a href="#">4</a>
<a href="#">Abbreviations and Acronyms.....</a>	<a href="#">4</a>
<b><a href="#">1 INTRODUCTION.....</a></b>	<b><a href="#">7</a></b>
<b><a href="#">1.1 Security Target and CC Identification.....</a></b>	<b><a href="#">7</a></b>
<b><a href="#">1.2 TOE Identification.....</a></b>	<b><a href="#">7</a></b>
<b><a href="#">1.3 TOE Type.....</a></b>	<b><a href="#">7</a></b>
<b><a href="#">1.4 TOE Overview.....</a></b>	<b><a href="#">7</a></b>
<a href="#">1.4.1 Required Hardware and Software.....</a>	<a href="#">8</a>
<a href="#">1.4.1.1 Java Virtual Machines.....</a>	<a href="#">8</a>
<a href="#">1.4.1.2 Browsers.....</a>	<a href="#">9</a>
<a href="#">1.4.1.3 LDAP.....</a>	<a href="#">9</a>
<a href="#">1.4.2 Intended Method of Use.....</a>	<a href="#">9</a>
<a href="#">1.4.3 Major Security Features.....</a>	<a href="#">10</a>
<b><a href="#">1.5 TOE Description.....</a></b>	<b><a href="#">10</a></b>
<a href="#">1.5.1 Product operation.....</a>	<a href="#">10</a>
<a href="#">1.5.1.1 WSP.....</a>	<a href="#">11</a>
<a href="#">1.5.1.2 Client-side.....</a>	<a href="#">12</a>
<a href="#">1.5.1.2.1 JWT connection.....</a>	<a href="#">13</a>
<a href="#">1.5.1.2.2 Web Server Gate operation of HTTP handler.....</a>	<a href="#">14</a>
<a href="#">1.5.1.3 HOBLink Security Manager.....</a>	<a href="#">14</a>
<a href="#">1.5.2 TOE boundaries.....</a>	<a href="#">14</a>
<a href="#">1.5.2.1 Physical.....</a>	<a href="#">14</a>
<a href="#">1.5.2.2 Logical.....</a>	<a href="#">15</a>
<a href="#">1.5.2.3 Configurations.....</a>	<a href="#">16</a>
<b><a href="#">2 CC CONFORMANCE CLAIM.....</a></b>	<b><a href="#">17</a></b>
<b><a href="#">3 SECURITY PROBLEM DEFINITION.....</a></b>	<b><a href="#">17</a></b>
<b><a href="#">3.1 Threat Environment.....</a></b>	<b><a href="#">17</a></b>
<a href="#">3.1.1 Assets.....</a>	<a href="#">17</a>
<a href="#">3.1.2 Threat Agents.....</a>	<a href="#">17</a>
<a href="#">3.1.3 Threats countered by the TOE.....</a>	<a href="#">18</a>
<a href="#">3.1.4 Threats countered by the TOE environment.....</a>	<a href="#">18</a>
<b><a href="#">3.2 Assumptions.....</a></b>	<b><a href="#">18</a></b>
<a href="#">3.2.1 Environment of use of the TOE.....</a>	<a href="#">18</a>
<a href="#">3.2.1.1 Physical.....</a>	<a href="#">18</a>
<a href="#">3.2.1.2 Personnel.....</a>	<a href="#">18</a>
<a href="#">3.2.1.3 Procedural.....</a>	<a href="#">19</a>
<a href="#">3.2.1.4 Connectivity.....</a>	<a href="#">19</a>
<b><a href="#">3.3 Organizational Security Policies.....</a></b>	<b><a href="#">20</a></b>
<b><a href="#">4 SECURITY OBJECTIVES.....</a></b>	<b><a href="#">20</a></b>
<b><a href="#">4.1 Objectives for the TOE.....</a></b>	<b><a href="#">20</a></b>
<b><a href="#">4.2 Objectives for the Operational Environment.....</a></b>	<b><a href="#">21</a></b>
<b><a href="#">4.3 Security Objectives Rationale.....</a></b>	<b><a href="#">22</a></b>
<a href="#">4.3.1 Coverage.....</a>	<a href="#">22</a>
<a href="#">4.3.2 Sufficiency.....</a>	<a href="#">23</a>
<b><a href="#">5 EXTENDED COMPONENTS DEFINITION.....</a></b>	<b><a href="#">27</a></b>
<b><a href="#">5.1 Class FMT: Security management.....</a></b>	<b><a href="#">28</a></b>
<a href="#">5.1.1 TOE Configuration (FMT_CFG).....</a>	<a href="#">28</a>
<a href="#">5.1.1.1 FMT_CFG.1 - Configuration of security functions.....</a>	<a href="#">28</a>
<a href="#">5.1.1.2 FMT_CFG.2 - Configuration value initialization.....</a>	<a href="#">29</a>
<b><a href="#">6 SECURITY REQUIREMENTS.....</a></b>	<b><a href="#">29</a></b>

<b>6.1 TOE Security Functional Requirements</b>	<b>29</b>
6.1.1 Information flow control policy models	30
6.1.1.1 Information flow control policy model (JWT)	30
6.1.1.2 Information flow control policy model (HTTPS)	31
6.1.1.3 Information flow control policy model (WSP)	31
6.1.2 Cryptographic support	32
6.1.2.1 Cryptographic key generation (FCS_CKM.1(RNG))	32
6.1.2.2 Cryptographic key generation (FCS_CKM.1(RSA))	32
6.1.2.3 Cryptographic key distribution (FCS_CKM.2)	33
6.1.2.4 Cryptographic key destruction (FCS_CKM.4)	34
6.1.2.5 Cryptographic operation (FCS_COP.1(TLS))	34
6.1.2.6 Cryptographic operation (FCS_COP.1(CERT))	35
6.1.2.7 Random number generation (Class DRG.3) (FCS_RNG.1)	35
6.1.3 JWT TLS connectivity	36
6.1.3.1 Subset information flow control (FDP_IFC.1(JWT))	36
6.1.3.2 Simple security attributes (FDP_IFF.1(JWT))	37
6.1.3.3 Basic internal transfer protection (FDP_ITT.1)	38
6.1.3.4 Integrity monitoring (FDP_ITT.3)	38
6.1.3.5 Configuration value initialization (FMT_CFG.2(JWT))	39
6.1.4 HTTPS connectivity	39
6.1.4.1 Subset information flow control (FDP_IFC.1(HTTPS))	39
6.1.4.2 Simple security attributes (FDP_IFF.1(HTTPS))	39
6.1.4.3 Configuration value initialization (FMT_CFG.2(HTTPS))	40
6.1.4.4 Inter-TSF trusted channel (FTP_ITC.1)	40
6.1.5 Identification, Authentication and Authorization	41
6.1.5.1 Complete information flow control (FDP_IFC.2)	41
6.1.5.2 Simple security attributes (FDP_IFF.1(WSP))	41
6.1.5.3 User attribute definition (FIA_ATD.1)	42
6.1.5.4 Timing of authentication (FIA_UAU.1)	42
6.1.5.5 Timing of identification (FIA_UID.1)	43
6.1.5.6 User-subject binding (FIA_USB.1)	43
6.1.5.7 Configuration value initialization (FMT_CFG.2(WSP))	43
6.1.5.8 Configuration of security functions (FMT_CFG.1)	44
<b>6.2 Security Functional Requirements Rationale</b>	<b>44</b>
6.2.1 Coverage	44
6.2.2 Sufficiency	45
6.2.3 Security requirements dependency analysis	46
<b>6.3 Security Assurance Requirements</b>	<b>48</b>
<b>6.4 Security Assurance Requirements Rationale</b>	<b>49</b>
<b>7 TOE SUMMARY SPECIFICATION</b>	<b>49</b>
<b>7.1 TOE Security Functionality</b>	<b>49</b>
7.1.1 Cryptographic primitives	50
7.1.1.1 General characteristics of the TLS protocol	50
7.1.1.2 TLS implementation in the TOE	50
7.1.2 Certificate Generation	51
7.1.3 Establishment and maintenance of TLS protected links	51
7.1.4 Identification, authentication and authorization	52
7.1.4.1 HTTP session cookies	52
<b>8 CONVENTIONS, TERMINOLOGY, AND ACRONYMS</b>	<b>55</b>
<b>8.1 Terminology</b>	<b>55</b>
<b>9 INDEX OF TABLES AND ILLUSTRATIONS</b>	<b>56</b>
<b>10 RELATED STANDARDS AND DOCUMENTS</b>	<b>57</b>
<b>11 APPENDIX/APPENDICES</b>	<b>60</b>
<b>11.1 Appendix A: Overview of HOB RD VPN scenario</b>	<b>60</b>



HOB RD VPN Software and Documentation 2005-2013 © HOB

All rights are reserved. Reproduction of editorial or pictorial contents without express permission is prohibited.

HOB RD VPN and HOBLink software and documentation have been tested and reviewed. Nevertheless, HOB will not be liable for any loss or damage whatsoever arising from the use of any information or particulars in, or any error or omission in, this document. HOB reserves the right to change the specification or parts of it without prior notice.

## Symbols and Conventions

This document uses certain symbols and conventions, which have the following meanings:

-  This symbol is used to indicate paragraphs with special informative character.
-  This symbol is used for procedures that may result in major changes. Please make sure that the results will correspond with your intentions.

- References to HOB RD VPN/HOBLink program commands and dialog boxes are printed in bold, e.g. Select the command **Open...**
- Keys or key combinations are put in square brackets, e.g. [space].
- Options and push buttons, selectable in a dialog box, are in printed bold, e.g. **user defined**.
- Cross-references to other chapters or figures are printed in italics and are accompanied by the symbol ►. The chapter and / or page number is also referenced.
- References to previous CC evaluations are printed in italics on a grey background, e.g. *interface 6*.

## Document history

Date	Version	Author	Changes
Jan. 2014	2.2		Version to be published

## Abbreviations and Acronyms

The following abbreviations and acronyms are used in this Security Target:

AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
FDP	Forms of user Data Protection
GUI	Graphical User Interface
HL	HOBLink
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol / Secured
IP	Internet Protocol

JNI	Java Native Interface
JRE	Java Runtime Environment
JVM	Java Virtual Machine
JWT	Java Windows Terminal
LAN	Local Area Network
MAC	Message Authentication Code
MD	Message Digest
OSP	Operational Security Policy
PKI	Public Key Infrastructure
PP	Protection Profile
RDP	Remote Desktop Protocol
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	HOB Security Manager
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification
URL	Uniform Resource Locator
WSG	Web Secure Gate
WSP	HOB WebSecureProxy

#### Trademarks

- Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
- UNIX is a registered trademark of The Open Group<sup>1</sup>.
- Microsoft Windows is a trademark of Microsoft Corporation.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates.
- All other product names, company names and service names may be trademarks, registered trademarks or service marks of their respective corporations or owners.

---

<sup>1</sup> See <http://www.unix.org/trademark.html>



# 1 Introduction

## 1.1 Security Target and CC Identification

ST title	Security Target for HOB RD VPN blue edition
ST version	2.2
Developer	HOB GmbH & Co. KG, Cadolzburg, Germany
CC version	Version 3.1, Revision 4
Certification ID	BSI-DSZ-CC-0832
Assurance level	EAL4, augmented by ALC_FLR.2

## 1.2 TOE Identification

	TOE Reference
TOE / Product name	HOB RD VPN blue edition
Product version	2.1 10.5397

## 1.3 TOE Type

The TOE is an encryption secured remote access solution (a so-called SSL-VPN) based on the TLSv1.1 [RFC4346] and TLSv1.2 [RFC5246] protocol.

## 1.4 TOE Overview

HOB RD VPN blue edition is a software package that provides TLS secured access to servers. In the evaluated configuration, it provides secured access to Remote Desktop servers as well as to web servers. The evaluated configuration of the product is built of three main components:

1. A gateway called “WebSecureProxy” located in front of the destination server (referred to as “WSP”). This software includes a module called “HTTP handler” that enables it to act as a web server gateway as well as an integrated web server. The WSP can handle all incoming connections over one single TCP/IP port. The WSP is equipped with a module called “HOBLink Secure, Server”<sup>2</sup> that performs all cryptographic operations on the server side.
2. A Java client application for Remote Desktop Services called “HOBLink JWT”. HOBLink JWT is equipped with a module called “HOBLink Secure, Client”, that performs all cryptographic operations on the client side. This component is located on the server within the RD VPN server installation and is downloaded by the client and executed on the client side.
3. An administrative tool called “HOBLink Security Manager” (Security Manager). It generates the HOBLink Security Units (each a set of files) containing the

<sup>2</sup> The identifiers “HOBLink Secure, Client” and “HOBLink Secure, Server” are formal definitions for a module called “HOBLink Secure SSL Software module”. This module is referred to hereinafter as “HOBLink Secure, Client” or “HOBLink Secure, Server” according to the role of the component it is used with. The “HOBLink Secure SSL Software module” is executed in different ways on the server-side and on the client-side. It uses identical code for cryptographic operations on both sides. The module is part of HOBLink Secure which is a software developed by HOB.

configurations and certificate(s) for the server and the client side. The HOB WSP employs the HOBLink Security Unit for the server and HOBLink JWT uses that for the client for establishing a secured communication. The administrator must transmit the generated units to the WSP in a secure manner. The files of the client HOBLink Security Unit are transmitted to the HOBLink JWT client via an already established TLS channel. The client unit is therefore protected for integrity, authenticity and privacy.

### 1.4.1 Required Hardware and Software

Table 1: Hardware and Software requirements

TOE component	Hardware requirements	Software requirements
HOBLink JWT (client software):	Intel Pentium Processor 1 GHz or CPU with equivalent or higher processing speed  256 Mbytes of RAM available	MS Windows 7  MS Windows 8  Apple Mac OS X 10.8 Intel 64-bit  openSUSE Linux 12.2 (with graphical subsystem installed)
WebSecureProxy (gateway):	Intel Pentium Processor 1 GHz or CPU with equivalent or higher processing speed  1 Gbytes of RAM available  250 ... 450 Mbytes of non-volatile storage space	SUSE Linux Enterprise Server 11 on Intel EM64T SP2
HOBLink Security Manager (administration workstation):	Intel Pentium Processor 1 GHz or CPU with equivalent or higher processing speed  256 Mbytes of RAM available  160 Mbytes of non-volatile storage space	see "HOBLink JWT (client software)" above

#### 1.4.1.1 Java Virtual Machines

The TOE component HOBLink Security Manager implicitly installs a third party JVM on Windows and Linux. The delivery of the JVM is mandatory on Linux and Windows, and this JVM is not shared with any other software, so it can be considered to be outside of the TOE. On Apple MAC OS X systems a Java Virtual Machine must already be installed before the HOBLink Security Manager is installed. The installer software requires a JVM that is downloaded from the Apple Mac OS X support web site. The following table contains the JVM versions that are used for the HOBLink Security Manager.

Table 2: JVMs that are currently used for the HOBLink Security Manager

OS family	JVM version
Windows	Sun Java 1.6.0 update 26 (32-bit)
Apple Mac OS X	Apple Java 1.6.0 update 65 (64-bit)

OS family	JVM version
Linux	Sun Java 1.6.0 update 26 (32-bit)

The HOBLink JWT component is a Java application and executes within the client's JVM of the installed JRE. The web browser starts the JVM (according to the configuration in the web browser) and passes necessary information to start HOBLink JWT. Recommended versions of web browsers are listed hereafter. HOBLink JWT runs on Java JVM versions listed in table 3, but the client side user is advised to use the most up-to-date versions provided by Oracle for security reasons.

**Table 3: JVMs allowed to be used with HOBLink JWT**

OS family	JVM version <sup>3</sup>
Windows	Oracle Java 1.7.0 update 45 (32-bit)
Apple Mac OS X	Oracle Java 1.7.0 update 45 (64-bit)
Linux	Oracle Java 1.7.0 update 45 (32-bit)

Note: The WebSecureProxy is not a Java software and does therefore not require a JVM.

#### 1.4.1.2 Browsers

Web browsers with the support for TLS v1.1 and TLS v1.2 are suitable for communication with the HTTP handler module. Browsers that currently support this requirement are, for example, Internet Explorer, Opera or Google Chrome.

#### 1.4.1.3 LDAP

The "WebSecureProxy" (WSP) uses an LDAP server to verify credentials and read other information as discussed in the subsequent sections.

WSP does not require a specific brand of LDAP server, but the LDAP server must support LDAPv3<sup>4</sup>.

### 1.4.2 Intended Method of Use

Users of the TOE start a browser on their client system and connect to the "WebSecureProxy" (WSP) server using the HTTPS protocol. The WSP server requests a username and password from the client that are verified with the user's credentials stored in an LDAP server. After a successful identification and authentication against an LDAP server, the user is granted access to Remote Desktop services (using the HOBLink JWT which is executed within a JVM) as well as web-based services (displayed by the client browser) protected by the TOE. Access to the Remote Desktop services or web-based services is granted by the WSP based on an access configuration applicable to the authenticated user.

The WSP implements a forwarding of the RDP data (messages) between the HOBLink JWT client and the protected Remote Desktop services.

<sup>3</sup> Java JRE 1.7 implicitly supports TLS v1.1 and TLS v1.2. The user must ensure that these TLS protocols are activated in the Java Control Panel.

<sup>4</sup> An implementation of parts of RFC 4510 and related documents is required for the performed LDAP database accesses.

To ensure a seamless access of web pages from the protected web-based services, the WSP implements an address-rewrite of the transmitted URLs as well as of the URLs found in the web pages to point to the WSP as gateway.

In the evaluated configuration, the communication is routed between the WSP and either the client browser or the HOBLINK JWT through an untrusted network. All of these communications are secured using the TLS protocol when in transit through the untrusted network – the communication between WSP and the client's browser or HOBLINK JWT is always routed through a TLS channel.

### 1.4.3 Major Security Features

The evaluated configuration of HOB RD VPN blue edition provides the following security services that are considered in this document:

- The TOE provides cryptographic primitives required to implement the TLS protocol, including symmetric and asymmetric key generation methods.
- The “Certificate Generation” service is provided by a utility for the generation of certificates and keys for use in TLS secured connections. This software is called “HOBLINK Security Manager”.
- The “TLS Protocol Function” is provided by the module “HOBLINK Secure SSL Software module”. The HOBLINK Secure SSL module implements the cryptographic primitives as well as the TLS protocol logic. Therefore, this module encrypts the HTTP or RDP data using the TLS protocol before sending it to the recipient via the untrusted network. In addition, this module also decrypts the received TLS data stream. The HOBLINK Secure SSL Software module is used by HOBLINK JWT as well as by the WSP. To distinguish both occurrences of this module, this Security Target uses the terms of “HOBLINK Secure, Client” for the instance integrated with HOBLINK JWT and “HOBLINK Secure, Server” for the instance integrated with WSP.
- The WSP requires the user to identify and authenticate before proceeding with any access request to a server. The WSP denies access to the protected resources without a successful identification and authentication. The WSP allows the administrator to specify role-based access lists. These access lists reference the protected HTTP or RDP servers a user is allowed or denied to connect to.

## 1.5 TOE Description

This section provides a product description in order to point out the purpose of the TOE and its possible fields of application. Furthermore, the scope of the evaluated configuration is defined.

### 1.5.1 Product operation

HOB RD VPN blue edition is a software package that provides TLS secured access to web servers and Remote Desktop servers. These servers are the resources protected by the TOE.

The evaluated configuration of the product is built of the following main components that work together to deliver the communication protection.

The following figure visualizes the systems and components involved, the physical boundary of the TOE, and shows relevant communication paths. The following sections explain the different TOE components. As the illustration may be hard to read, it is presented in a larger

scale in section 11.1.

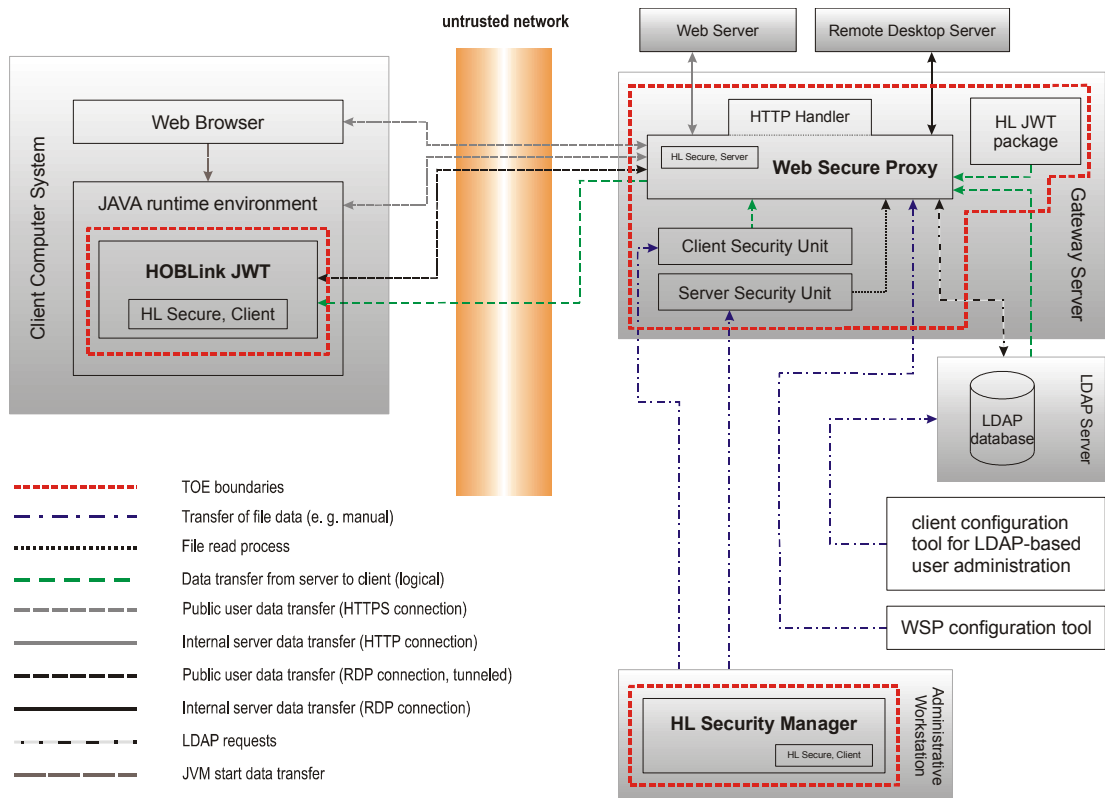


Fig. 1: Overview of HOB RD VPN scenario

### 1.5.1.1 WSP

The WSP reads its configuration and the server HOBLink Security Unit during start up. The data of each file of the server HOBLink Security Unit are passed to “HOBLink Secure, Server”. The WSP accepts incoming encrypted requests, ensures the identification and authentication of the user via username and password and generates a start web page with URLs (so-called links) to the web servers and Remote Desktop servers the user is allowed to access.

The username and password are validated with an LDAP server.

The start web page is dynamically created for each user based on the master copy web page stored in a folder of the HOB RD VPN installation and according to the settings found in the WSP configuration and the Web Server Gate (WSG) configuration. These Web Server Gate settings are stored in LDAP for this user.

The list of servers authorized for use by the user are specified in the WSP configuration file. There is a list for each of the web servers and the Remote Desktop servers. The list for the Remote Desktop servers works as a so-called white list, while the list for the web servers can work as a white list or as a black list. The WSP configuration can contain these lists with a global part and a role-based part. Authorization for the access of the users to allowed servers depends on the role assigned to the users.

When a user connects to the WSP, the WSP generates an HTTP session cookie after a successful authentication and returns it to the calling browser. This cookie must be presented by the user browser for each HTTP request. In addition, when establishing an RDP session

HOBLink JWT must transmit the ticket information of the cookie to the WSP to allow the WSP assign the new connection to the already authenticated user. Note: even if a user knows other URLs to protected servers (either web or Remote Desktop servers) that are located in the "in-house" area and are not listed on the user's start web page, the WSP does not allow access to this server if the WSP configuration excludes this user from the group of authorized users or does not include the user in this group.

The WSP mediates access to:

- the WSP-integrated web server (part of the TOE), by accepting the HTTPS requests. The integrated web server (which is a module of the "HTTP handler") of the WSP involved in this operation ensures that the user credentials are passed to the authentication method and that a unique cookie for each HTTP session is created and assigned to a user.
- a protected web server by unwrapping the HTTP requests from the received TLS requests. The WSP establishes an unencrypted connection to the destination server system. The processing of the TLS protocol enforced for data in transit between the WSP and the client web browser is performed by "HOBLink Secure, Server". Destination servers are only available to users if they are previously defined in the WSP configuration. Additionally, the Web Server Gate configuration of a specific user that is read from LDAP defines the start web page for this user. The WSP ensures that any link on the back-end web site is rerouted through the WSP.
- a protected RDP server by unwrapping the RDP requests from the received TLS requests. The WSP establishes an unencrypted connection to the destination server system. The processing of the TLS protocol enforced for data in transit between the WSP and HOBLink JWT is performed by "HOBLink Secure, Server". Destination servers are only available to users if they are previously defined in the WSP configuration. Additionally, the Web Server Gate configuration of a specific user that is read from LDAP defines the start web page for this user.
- the JWT configuration of a specific user read from LDAP. This configuration determines the window GUI and user specific properties such as the keyboard features or language for the RDP session and the peripheral components that are available from within the RDP session. Note: the WSP only allows the establishment of a new RDP communication link using the ticket information of the above mentioned HTTP cookie that HOBLink JWT must present to the WSP.

A start web page is dynamically created for each user displaying the links to the authorized servers based on the access control list applicable to the user. In addition, the layout parameter settings for the link page are found in the Web Server Gate configuration stored in LDAP for this user.

#### 1.5.1.2 Client-side

The user starts a browser on the client system, provides the destination URL and initiates a connection to the WSP. The user must establish trust in the server certificate offered by the WSP it connects to, but which is outside this evaluation. This can be established by loading the WSP root certificate onto the client system (e.g. into the browser or the operating system key store) to allow the browser to validate the certificate offered by the WSP. A similar approach must be claimed for the JRE.

After connecting to the WSP, the user has to identify and authenticate via a username and password. The user credentials are matched with the credentials stored in an LDAP server. The WSP performs an LDAP-bind operation to verify the credentials, which implies that the identification and authentication decision is performed by the LDAP server and the WSP enforces the decision made by the LDAP server.

The WSP-integrated web server provides a web page together with a unique cookie after a successful authentication. This page contains the URLs to protected web servers as well as links to those protected Remote Desktop servers the user is authorized to access.

The currently established HTTPS session with its cookie continues to be used when accessing protected web servers.

When accessing a Remote Desktop server, the selected URL causes the Java application of "HOBLink JWT" to be downloaded. HOBLink JWT is stored as the HL JWT package in a folder of the RD VPN installation. The package contains the Java jar-file and additional JNI executables that are used to provide native, OS-dependent functions to the Java application. HOBLink JWT is executed as a Java Webstart application on the client system.

#### 1.5.1.2.1 JWT connection

As mentioned above, HOBLink JWT is downloaded by selecting a link to a Remote Desktop server on the start web page presented by the WSP. Selecting such a link triggers the browser to start a HTTPS secured connection to the destination address and downloads the HOBLink JWT Webstart file. The HTTP session cookie is used to authenticate the connections with the WSP to allow the WSP to assign the new connection to the already authenticated user. The HOBLink JWT Webstart file as provided by the link on the WSP-generated web start page contains the destination address, the HTTP session cookie, the client HOBLink Security Unit and a unique identification for the user's JWT configuration that will be downloaded from the server component of RDVPN. The client HOBLink Security Unit is stored in a folder of the HOB RD VPN installation (on the server) and is defined in the WSP configuration. In addition, the HOBLink JWT Webstart file points to the HOBLink JWT package (symbolized as "HL JWT package" in figure ► [Fig. 1: Overview of HOB RD VPN scenario](#)) that is to be downloaded by the JVM and that implements the client-side logic ensuring a secured data tunneling for RDP.

After the download of the HOBLink JWT package and its startup, HOBLink JWT establishes a new connection to the WSP and the "HOBLink Secure, Client" module initiates a new TLS handshake to "HOBLink Secure, Server" within the WSP.

All subsequent data exchanges are tunneled through this new TLS secured connection. During the establishment of the TLS link, the "HOBLink Secure, Client" module performs a server certificate validation using the root certificate or certificate chain found in the client HOBLink Security Unit already obtained.

To allow the WSP to assign the newly instantiated TLS connection to the already authenticated user, HOBLink JWT passes the information of the obtained HTTP session cookie<sup>5</sup> to the WSP. The WSP now uses this information for user authentication and after a successful verification the connection is continued or terminated if not successful. The WSP transfers data between HOBLink JWT on the client side through the newly established TLS channel and the selected Remote Desktop server in the protected environment.

After the successful establishment of the TLS link, a new window is presented that allows the user to enter the credentials needed to access the requested Remote Desktop server. These credentials are forwarded to the Remote Desktop server with the intention of allowing this server to perform the identification and authentication of the user based on these credentials. HOBLink JWT now uses the RDP protocol communication for the Remote Desktop session tunneled through the established TLS tunnel and displays the corresponding remote desktop GUI.

---

<sup>5</sup> Please note that the session ticket, the user name and the domain name that are embedded in the HTTP session cookie are used for the mentioned authentication process.



### 1.5.1.2.2 Web Server Gate operation of HTTP handler

The user clicks on a link to a protected web server on the start page offered by the WSP. The WSP establishes the communication with the protected web server and forwards the HTTP requests from the client web browser to the web server. The replies of the web server are also forwarded to the client web browser using the HTTPS communication channel that is already established with the initial HTTPS request of the client browser.

The user HTTP session cookie is used to authenticate the requests in the WSP. All HTTP requests and links within HTML pages are modified by the Web Server Gate within the WSP to reroute these addresses from the browser to the Web Server Gate and from there via WSP to the web server and back.

### 1.5.1.3 HOBLink Security Manager

The administrative tool "HOBLink Security Manager" (Security Manager) is used to generate the HOBLink Security Units. A HOBLink Security Unit is a set of files containing the configurations and certificates for the server and the client sides.

The HOBLink Security Manager implements the mechanism to generate asymmetric keys to support the TLS protocol.

The HOBLink Security Manager includes the HOBLink Secure SSL Software module and uses the certificate generation, the random number generator and other functions. It can be seen that the HOBLink Security Manager does not explicitly use the functionality for server or client as needed by the components involved in the secured communication. The HOBLink Secure SSL Software module that it uses includes only those same classes as used in HOBLink JWT. Therefore "HL Secure, Client" is added to the HOBLink Security Manager in figure ► [Fig. 1: Overview of HOB RD VPN scenario](#). The HOBLink Security Manager itself does not require server specific or client specific functions.

## 1.5.2 TOE boundaries

Figure ► [Fig. 1: Overview of HOB RD VPN scenario](#) shows the physical and logical boundaries of the TOE. The following table provides a short description of the software components for the evaluation.

### 1.5.2.1 Physical

The following software components form the TOE:

Table 4: Software components of the TOE

Component	Purpose
WebSecureProxy	<p>A multi-functional gateway that translates the encrypted data stream from the public side of the network into "clear-text" communication for the internal LAN and vice versa.</p> <p>The cryptographic operations are performed by the module "HOBLink Secure, Server".</p> <p>The module "HTTP Handler" contains the functions "Web Server Gate" and "integrated web server" that provide additional web server gateway and web server functionality.</p>



Component	Purpose
HOBLink Security Manager	An offline PKI utility designed to create, import, export and maintain X.509v3 certificates and TLS configurations required for the TLS and HTTPS connections.
HOBLink JWT	A Java application for Remote Desktop Services. Its purpose is to show the GUI of a session to a Remote Desktop server on the local workstation.  It includes a module called "HOBLink Secure, Client" that performs the cryptographic operations.

The HOB RD VPN blue edition product media contains additional software that can be used with the WSP or in the environment the WSP is used. This additional software allows, for example, alternative protocols or alternative authentication methods to be used. All the additional software is not part of the TOE and does not provide security services relevant to the context of this document.

Along with the TOE components mentioned above, HOB provides a number of tools that fulfill the requirements to create and edit specific HOB RD VPN blue edition configurations. This includes the configurations for TOE relevant components and also the configurations for the additional software on the product media. The manual also provides information to analyze most configuration files, if the files are human readable.

The configuration tools and software used to view or edit configuration files does not belong to the TOE and therefore will not be discussed further.

The following guidance is delivered together with the TOE:

- Administration Guide HOBLink Secure and HOBLink Security Manager
- Administration Guide HOB Remote Desktop VPN blue edition

### 1.5.2.2 Logical

The primary security features of the TOE are:

- Cryptographic primitives required to implement the TLS protocol, including symmetric and asymmetric key generation methods. To support the cryptographic primitives, a deterministic random number generator is provided which is based on the CTR\_DRBG design with an AES-128 core specified in the NIST SP800-90A documentation.
- RSA certificate and RSA key generation provided by the HOBLink Security Manager to support the TLS protocol handshake.
- Establishment and maintenance of TLS protected links. These links can transport HTTP requests as well as the RDP protocol. The TLS protocol implementation provided by the web browser and by the JVM in the JRE is not part of the TOE however it is enforced by the TOE component of the WSP.
- Enforcement of the identification and authentication decisions performed by the LDAP server before users can access any resources protected by the TOE. In addition, the TOE implements a role-based access control. Each user can be given or denied access to a protected resource of:

- web servers,
  - Remote Desktop servers.
- Mechanisms to configure the security functions are offered by the TOE.

The TOE provides many more functions and mechanisms. The evaluation ensures that all these additional functions do not interfere with the above mentioned security mechanisms in the evaluated configuration of the TOE. Mechanisms and functions that would interfere with the operation of the security functions are disallowed in the evaluated configuration. The section of the administrator guidance discussing the specific configuration of the product to conform to the Common Criteria evaluation provides instructions to the administrator on how to disable them. Note: TOE mechanisms which provide additional restrictions to the above claimed security functions are allowed in the TOE's evaluated configuration.

The WSP and HOBLink JWT are administered by configuration files which constitute the management interface. The Security Manager is a utility to generate among others configuration files i.e. the HOBLink Security Units for the Server and Client. It does not enforce any form of roles.

Note: Software and mechanisms not covered with security claims and subsequent assessments during the evaluation or disabling of the respective functionality in the evaluated configuration result from resource constraints during the evaluation, but does not imply that the respective package or functionality is implemented insecurely.

### 1.5.2.3 Configurations

Before any TLS connections can be established, the administrator must generate the configuration for the "WebSecureProxy" server. The guidance documents the contents of the configuration file.

In addition, before any TLS connection can be established, the administrator creates two HOBLink Security Units, one for the "HOBLink Secure, Client" and one for the "HOBLink Secure, Server". Each "HOBLink Security Unit" is a set of files and consists of the following three files:

- the configuration file,
- the certificate database file,
- and the password file holding the password that protects access to the configuration file and to the certificate database file.

Both HOBLink Security Units are manually and securely distributed to the WSP by means outside the TOE. The guidance documents the directory structure which hosts the files for the server and client side. When the client requests the initiation of a Remote Desktop session, the client downloads the HOBLink JWT Java application and the client HOBLink Security Unit via the already established HTTPS channel.

Furthermore, a configuration file for the client software "HOBLink JWT" has to be created. This configuration file mainly defines a set of presentation parameters such as the display size. The configuration parameters specified in this configuration file are not relevant to the enforcement of the security claims made in this Security Target. The administrator stores the configuration information in the LDAP tree, either on a per-user basis or on a per-group basis.

All configuration files are generated and maintained with tools that are not part of this TOE. All configuration parameters that are intended to be used in the configuration files are documented in the manual.

During the initial installation, an OpenDJ LDAP server is additionally installed on the server system. An administrative tool exists that allows the configuration of the HOB WSP with GUI support if a manually edited and reviewed configuration is not to be used. The OpenDJ LDAP system and the configuration GUI tool are not part of the TOE. Therefore, the LDAP server is unused in the evaluated configuration except in the case of a severe configuration error.

## 2 CC Conformance Claim

This ST is CC Part 2 extended and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL4, augmented by ALC\_FLR.2.

This ST does not claim conformance to any Protection Profile:

Common Criteria [CC] version 3.1 revision 4 is the basis for this conformance claim.

## 3 Security Problem Definition

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 protection within the TOE or its environment is required.
- Any organisational 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 for which the TOE is intended.

### 3.1 Threat Environment

Threats to be countered by the TOE are characterized by the combination of an asset being subject to a threat, a threat agent and an adverse action.

#### 3.1.1 Assets

The assets in transit to be protected are TSF and user data transmitted between physically separated parts of the TOE over an untrusted network.

The resource assets to be protected are the web servers and RDP servers the WSP mediates access to.

#### 3.1.2 Threat Agents

The threat agents are attackers who have access to the untrusted network and who have the ability and skill to monitor, modify, delete, re-play or re-order transmitted information or to insert information into the transmitted information. Attackers are assumed to have an enhanced-basic attack potential.

### 3.1.3 Threats countered by the TOE

Table 5: Threats to be countered by the TOE

Threat	Description
T.Access.Resource	A threat agent might gain access to the resources of web servers and Remote Desktop servers protected by the WSP without being appropriately authorized according to the TOE security policy.
T.IA.Masquerade	A threat agent might masquerade as an authorized entity including the TOE itself or a part of the TOE in order to gain unauthorized access to resources of web servers and Remote Desktop servers protected by the WSP.
T.IA.User	A threat agent might gain access to resources of web servers and Remote Desktop servers protected by the WSP without being identified and authenticated.
T.Untrusted-Path	A threat agent may attempt to disclose, modify, delete, re-play, re-order or insert TSF and/or user data by monitoring, modifying, deleting, re-playing or re-ordering the information transmitted over the untrusted network or by inserting additional information in the transmitted information in an unnoticeable manner.

### 3.1.4 Threats countered by the TOE environment

There are no threats to be solely addressed by the operational environment.

## 3.2 Assumptions

### 3.2.1 Environment of use of the TOE

#### 3.2.1.1 Physical

Table 6: Assumptions to be covered by physical constraints

Assumption	Description
A.Physical	It is assumed that the environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

#### 3.2.1.2 Personnel

Table 7: Assumptions to be covered by personnel constraints

Assumption	Description
A.Administrators	The TOE environment is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance

Assumption	Description
	documentation.
A.AuthUser	Authorized users possess the necessary authorization to access at least some of the resources protected by the TOE and are expected to act in a cooperating manner in a benign environment.
A.TrainedUser	Users are sufficiently trained to use the TOE in a secure manner.

### 3.2.1.3 Procedural

Table 8: Assumptions to be covered by procedural constraints

Assumption	Description
A.DestroyRSA	RSA keys stored in non-volatile storage are securely destroyed when they are no longer needed.
A.LDAPMgt	The LDAP server is assumed to be under the same management control, operating under the same security policy constraints and having the same level of physical protection as the TOE.
A.LDAPFunc	The LDAP server is assumed to correctly implement the functionality required by the TSF consistent with the assumptions defined for this functionality, i.e.: <ul style="list-style-type: none"> <li>correctly perform the I&amp;A decision requested via an LDAP-bind operation by the TOE (WSP),</li> <li>protect the user credentials against brute force attacks<sup>6</sup>,</li> <li>supporting LDAPv3 protocol for accessing the directory services.</li> </ul>
A.Systems	The operating systems, the Java virtual machines, and the web browser operate according to their specification. These external systems are configured in accordance with the installation guidance and the evaluated configuration guidance of the TOE. These systems are assumed to be well managed and trustworthy.
A.Time	The underlying operating system provides reliable time information to the TOE.

### 3.2.1.4 Connectivity

Table 9: Assumptions to be covered by connectivity constraints

Assumption	Description
A.ProtectedResources	Any connection between the untrusted network and the protected resources of web servers and Remote Desktop

<sup>6</sup> Techniques such as login authentication delay, account lockout after consecutive unsuccessful login attempts, password complexity rules, etc. can be used to implement this requirement.

Assumption	Description
	servers is established via the WSP by an appropriate network architecture.
A.SecMgr	The Security Manager is installed on a separate machine that is not physically connected to any network and the HOBLINK Security Units generated by this tool are transferred securely to the WSP.
A.WSP	The WebSecureProxy is installed on a separate machine without unprivileged users having local access and that does not host any productive relevant services such as database servers or alternative web servers besides the software that is provided through the HOB product installation. The logical access to this machine is restricted to authorized administrators.

### 3.3 Organizational Security Policies

Table 10: Organizational Security Policies to be met by the TOE

Assumption	Description
P.Certificates	The RSA keys and certificates are generated by the TOE facilities.

## 4 Security Objectives

This section identifies the security objectives for the TOE and for the TOE environment.

### 4.1 Objectives for the TOE

Table 11: Security Objectives for the TOE

Objective	Description
O.Certificates	The TOE provides the facility to generate RSA certificates and the corresponding keys.
O.Crypto.Net	The TSF must be designed and implemented in a manner that allows for establishing a trusted channel between distributed parts of the TOE that protects the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system.
O.I&A	The TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only.

Objective	Description
O.Resource.Access	The TSF must control access of subjects and/or users to the resources of web servers and Remote Desktop servers based on identity of the user. The TSF must provide authorized users with the means to specify which users/subjects are allowed to access a specific named object in that access mode.

## 4.2 Objectives for the Operational Environment

Table 12: Security Objectives for the TOE environment

Objective	Description
OE.Administrators	Those responsible for the TOE environment are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
OE.LDAP	<p>The LDAP server must implement the functionality required by the TSF correctly and provides its result to the TOE supporting LDAPv3. In particular the LDAP server must correctly perform the I&amp;A decision supported by the protection against brute forcing account credentials requested via an LDAP-bind operation by the TOE (WSP).</p> <p>The LDAP server must be under the same management control, operating under the same security policy constraints and must have the same level of physical protection as the TOE.</p>
OE.InfoProtect	<p>Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular:</p> <ul style="list-style-type: none"> <li>• Users are authorized to access parts of the data managed by the TOE and are trained to use the TOE in a secure manner in a benign environment.</li> <li>• Any connection between the untrusted network and the protected resources of web servers and Remote Desktop servers must be established via the WSP by an appropriate network architecture.</li> </ul>
OE.Install	Those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE.
OE.WSP	Those responsible for the TOE, install the WebSecureProxy on a separate machine without unprivileged users having local access and that does not host any productive relevant services such as database servers or alternative web servers

Objective	Description
	besides the software that is provided through the HOB product installation. The logical access to this machine is restricted to authorized administrators.
OE.Physical	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.
OE.DestroyRSA	Those responsible for the TOE must assure that RSA keys maintained with the HOBLink Security Units are securely destroyed when they are no longer needed.
OE.SecMgr	Those responsible for the TOE must assure that the Security Manager is installed on a separate machine that is not physically connected to any network and that the HOBLink Security Units generated by this tool are transferred securely to the WSP.
OE.System	Those responsible for the TOE must ensure that the operating systems, the Java virtual machines, and the web browser are installed and configured in accordance with the guidance of the TOE and that these mechanisms operate as specified. These systems are well managed and trustworthy. This also covers that only the software enumerated in this ST are used as underlying platform to ensure that proper date and time information is available.

### 4.3 Security Objectives Rationale

#### 4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

**Table 13: Mapping of security objectives to threats and policies**

Objective	Threats / OSPs
O.Certificates	P.Certificates
O.Crypto.Net	T.Untrusted-Path
O.I&A	T.IA.Masquerade, T.IA.User
O.Resource.Access	T.Access.Resource

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.



**Table 14: Mapping of security objectives for the Operational Environment to assumptions, threats and policies**

<b>Objective</b>	<b>Assumptions / Threats / OSPs</b>
OE.Administrators	A.Administrators
OE.LDAP	A.LDAPMgt, A.LDAPFunc, T.IA.User, T.IA.Masquerade
OE.InfoProtect	A.AuthUser, A.TrainedUser, A.ProtectedResources
OE.Install	A.Administrators
OE.WSP	A.WSP
OE.Physical	A.Physical
OE.DestroyRSA	A.DestroyRSA
OE.SecMgr	A.SecMgr
OE.System	A.Systems, A.Time

### 4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat:

**Table 15: Sufficiency of objectives countering threats**

<b>Threat</b>	<b>Rationale for security objectives</b>
T.Access.Resource	<p>The threat of accessing the resources of web servers and Remote Desktop servers protected by the WSP without being appropriately authorized according to the TOE security policy is removed by:</p> <ul style="list-style-type: none"> <li>• O.Resource.Access requiring the TSF to control access of subjects and/or users to the resources of web servers and Remote Desktop servers based on identity of the user. The TSF must provide authorized users with the means to specify which users/subjects are allowed to access a specific named object in that access mode.</li> </ul>
T.IA.Masquerade	<p>The threat of masquerading as an authorized entity including the TOE itself or a part of the TOE in order to gain unauthorized access to resources of web servers and Remote Desktop servers protected by the WSP is removed by:</p> <ul style="list-style-type: none"> <li>• O.I&amp;A requiring the TOE to ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only.</li> </ul>

Threat	Rationale for security objectives
T.IA.User	<ul style="list-style-type: none"> <li>• OE.LDAP requiring that the LDAP server correctly performs the requested I&amp;A decision, operating under the same security policy constraints as the TOE, having the same level of physical protection as the TOE and requiring the same management control as for the TOE.</li> </ul> <p>The threat of gaining access to resources of web servers and Remote Desktop servers protected by the WSP without being identified and authenticated is removed by:</p> <ul style="list-style-type: none"> <li>• O.I&amp;A requiring the TOE to ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only.</li> <li>• OE.LDAP requiring that the LDAP server correctly performs the requested I&amp;A decision, operating under the same security policy constraints as the TOE, having the same level of physical protection as the TOE and requiring the same management control as for the TOE.</li> </ul>
T.Untrusted-Path	<p>The threat of attempting to disclose, modify, delete, re-play, re-order or insert user data by monitoring, modifying, deleting, re-playing or re-ordering the information transmitted over the untrusted network or by inserting additional information in the transmitted information in an unnoticeable manner is removed by:</p> <ul style="list-style-type: none"> <li>• O.Crypto.Net requiring the TSF to be designed and implemented in a manner that allows for establishing a trusted channel between distributed parts of the TOE that protects the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system.</li> </ul>

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported:

**Table 16: Sufficiency of objectives holding assumptions**

Assumption	Rationale for security objectives
A.Physical	<p>The assumption that the environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE is covered by:</p> <ul style="list-style-type: none"> <li>• OE.Physical requiring that those responsible for the TOE must ensure that those parts of the TOE critical</li> </ul>

Assumption	Rationale for security objectives
A.Administrators	<p>to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.</p> <p>The assumption that the TOE environment is managed by one or more competent individuals. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation is covered by:</p> <ul style="list-style-type: none"> <li>• OE.Administrators requiring that those responsible for the TOE environment are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.</li> <li>• OE.Install requiring that those responsible for the TOE must establish and implement procedures to ensure that the hardware, software and firmware components that comprise the system are distributed, installed and configured in a secure manner supporting the security mechanisms provided by the TOE.</li> </ul>
A.AuthUser	<p>The assumption that authorized users possess the necessary authorization to access at least some of the resources protected by the TOE and are expected to act in a cooperating manner in a benign environment is covered by:</p> <ul style="list-style-type: none"> <li>• OE.InfoProtect requiring that users are authorized to access parts of the data managed by the TOE.</li> </ul>
A.TrainedUser	<p>The assumption that users are sufficiently trained to use the TOE in a secure manner is covered by:</p> <ul style="list-style-type: none"> <li>• OE.InfoProtect requiring that users are trained to use the TOE in a secure manner.</li> </ul>
A.DestroyRSA	<p>The assumption that RSA keys stored in non-volatile storage are securely destroyed when they are no longer needed is covered by:</p> <ul style="list-style-type: none"> <li>• OE.DestroyRSA requiring that those responsible for the TOE must assure that RSA keys maintained with the HOBLink Security Units are securely destroyed when they are no longer needed.</li> </ul>
A.LDAPMgt	<p>The assumption that the LDAP server is under the same management control, operating under the same security policy constraints and having the same level of physical protection as the TOE. is covered by:</p>

Assumption	Rationale for security objectives
A.LDAPFunc	<ul style="list-style-type: none"> <li>• OE.LDAP requiring the LDAP server to be under the same management control, operating under the same security policy constraints and having the same level of physical protection as the TOE.</li> </ul> <p>The assumption that the LDAP server correctly implements the functionality required by the TSF and provide it to the TOE consistent with the assumptions defined for this functionality, i.e.:</p> <ul style="list-style-type: none"> <li>• correctly perform the I&amp;A decision requested via an LDAP-bind operation by the TOE (WSP),</li> <li>• protect the user credentials against brute force attacks,</li> <li>• supporting LDAPv3 protocol for accessing the directory services.</li> </ul> <p>is covered by:</p> <ul style="list-style-type: none"> <li>• OE.LDAP requiring that the LDAP server correctly performs the I&amp;A decision supported by the protection against brute forcing account credentials requested via an LDAP-bind operation by the TOE (WSP) supporting LDAPv3.</li> </ul>
A.Systems	<p>The assumption that the operating systems, the Java virtual machines, and the web browser operate according to their specification. These external systems are configured in accordance with the installation guidance and the evaluated configuration guidance of the TOE and are assumed to be well managed and trustworthy is covered by:</p> <ul style="list-style-type: none"> <li>• OE.System requiring that those responsible for the TOE must ensure that the operating systems, the Java virtual machines, and the web browser are installed and configured in accordance with the guidance of the TOE and that these mechanisms operate as specified and are well managed and trustworthy.</li> </ul>
A.Time	<p>The assumption that the underlying operating system provides reliable time information to the TOE is covered by:</p> <ul style="list-style-type: none"> <li>• OE.System requiring that only the software enumerated in this ST are used as underlying platform to ensure that proper date and time information is available.</li> </ul>
A.ProtectedResources	<p>The assumption that any connection between the untrusted network and the protected resources of web servers and Remote Desktop servers is established via the WSP by an appropriate network architecture is implemented by:</p> <ul style="list-style-type: none"> <li>• OE.InfoProtect requiring that any connection between the untrusted network and the protected resources of web servers and Remote Desktop</li> </ul>

Assumption	Rationale for security objectives
A.SecMgr	<p>servers must be established via the WSP by an appropriate network architecture.</p> <p>The assumption that the Security Manager is installed on a separate machine that is not physically connected to any network and the HOBLink Security Units generated by this tool are transferred securely to the WSP is covered by:</p> <ul style="list-style-type: none"> <li>• OE.SecMgr requiring that those responsible for the TOE must assure that the Security Manager is installed on a separate machine that is not physically connected to any network and that the HOBLink Security Units generated by this tool are transferred securely to the WSP.</li> </ul>
A.WSP	<p>The assumption that the WebSecureProxy is installed on a separate machine without unprivileged users having local access to the machine and that does not host any productive relevant services such as database servers or alternative web servers besides the software that is provided through the HOB product installation is covered by:</p> <ul style="list-style-type: none"> <li>• OE.WSP requiring that those responsible for the TOE install the WebSecureProxy on a separate machine without unprivileged users having local access and that does not host any productive relevant services such as database servers or alternative web servers besides the software that is provided through the HOB product installation. The logical access to this machine is restricted to authorized administrators.</li> </ul>

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy, that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented:

**Table 17: Sufficiency of objectives enforcing Organizational Security Policies**

OSP	Rationale for security objectives
P.Certificates	<p>The policy that the RSA keys and certificates are generated by the TOE facilities is implemented by:</p> <ul style="list-style-type: none"> <li>• O.Certificates requiring the TOE to provide the facility to generate RSA certificates and the corresponding keys.</li> </ul>

## 5 Extended Components Definition

The ST claims the following extended components:

- FCS\_RNG.1

- FMT\_CFG.1
- FMT\_CFG.2

The SFR FCS\_RNG.1 is derived from [KS2011].

The TOE does not support administrative roles in the evaluated configuration, as this is handled in the TOE environment. The TOE is managed by configuration files. To better model this, the family CFG is introduced in class FMT instead of using FMT\_MSA/FMT\_SMF.

## 5.1 Class FMT: Security management

### 5.1.1 TOE Configuration (FMT\_CFG)

#### Family behavior

This family defines requirements for TOE configurations that are independent of administrative roles.

#### Component leveling

FMT\_CFG.1 specifies configurability of the TOE without the need of management roles.

FMT\_CFG.1 is not hierarchical to any other component within the FMT\_CFG family.

FMT\_CFG.2 specifies TOE configuration value initialization.

FMT\_CFG.2 is not hierarchical to any other component within the FMT\_CFG family.

#### Management: FMT\_CFG.1

There are no management activities foreseen.

#### Management: FMT\_CFG.2

There are no management activities foreseen.

#### Audit: FMT\_CFG.1

The following actions should be auditable if FAU\_GEN Security audit data generation is included in the PP/ST:

- Minimal: Changes of the TOE configuration.

#### Audit: FMT\_CFG.2

There are no audit events foreseen.

#### 5.1.1.1 FMT\_CFG.1 - Configuration of security functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT\_CFG.1.1 The TSF shall be capable of configuring the following security functions: [assignment: list of functions to be configurable by the TSF].

### Rationale

The configuration of the TOE is specified with a configuration method that is not dependent on TOE supported roles.

#### 5.1.1.2 FMT\_CFG.2 - Configuration value initialization

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT\_CFG.2.1 The TSF shall enforce the [assignment: access control SFP, information flow control SFP] to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT\_CFG.2.2 The TSF shall support the specification of alternative initial values to override the default values used in enforcing the security policy.

### Rationale

The defaults of the TOE configuration are specified with a configuration method that is not dependent on TOE supported roles.

## 6 Security Requirements

### 6.1 TOE Security Functional Requirements

The following table shows the Security functional requirements for the TOE, and the operations performed on the components according to CC part 2: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Table 18: Security functional requirements for the TOE

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
Crypto. Support	FCS_CKM.1(RNG)	FCS_CKM.1	[CC]	X	X	X	
	FCS_CKM.1(RSA)	FCS_CKM.1	[CC]	X		X	
	FCS_CKM.2	FCS_CKM.2	[CC]		X	X	
	FCS_CKM.4	FCS_CKM.4	[CC]			X	
	FCS_COP.1(TLS)	FCS_COP.1	[CC]	X	X	X	
	FCS_COP.1(CERT)	FCS_COP.1	[CC]	X	X	X	
	FCS_RNG.1	FCS_RNG.1	[KS2 011]		X	X	X
JWT TLS	FDP_IFC.1(JWT)	FDP_IFC.1	[CC]	X		X	
	FDP_IFF.1(JWT)	FDP_IFF.1	[CC]	X		X	

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
HTTPS	FDP_ITT.1	FDP_ITT.1	[CC]			X	X
	FDP_ITT.3	FDP_ITT.3	[CC]			X	
	FMT_CFG.2(JWT)	FMT_CFG.2	ECD	X		X	X
	FDP_IFC.1(HTTPS)	FDP_IFC.1	[CC]	X		X	
	FDP_IFF.1(HTTPS)	FDP_IFF.1	[CC]	X		X	
	FMT_CFG.2(HTTPS)	FMT_CFG.2	ECD	X		X	X
I&A and Auth.	FTP_ITC.1	FTP_ITC.1	[CC]		X	X	X
	FDP_IFC.2	FDP_IFC.2	[CC]			X	
	FDP_IFF.1(WSP)	FDP_IFF.1	[CC]	X		X	
	FIA_ATD.1	FIA_ATD.1	[CC]			X	
	FIA_UAU.1	FIA_UAU.1	[CC]			X	
	FIA_UID.1	FIA_UID.1	[CC]			X	
	FIA_USB.1	FIA_USB.1	[CC]			X	
	FMT_CFG.2(WSP)	FMT_CFG.2	ECD	X		X	X
	FMT_CFG.1	FMT_CFG.1	ECD			X	

## 6.1.1 Information flow control policy models

### 6.1.1.1 Information flow control policy model (JWT)

The security policy for the JWT TLS information flow control policy is defined by the security functional requirements in section 6.1.3. The following is a list of the subjects and resources participating in the policy.

- Subject:
  - HOBLink JWT component acting as the client
  - WSP component acting as the server
- Information security attribute:
  - Established TLS connection for each X.509 certificate:
    - Digital signature generated with the X.509 certificate,
    - Distinguished Name (DN) stored in an X.509 certificate,
    - Validity period of X.509 certificate,
    - BasicConstraints
- Resources:
  - Protected Remote Desktop servers;



- Operation:
  - all data transmissions between the HOBLink JWT component and the WSP component
- User data:
  - All RDP data exchanged between the resources managed by the WSP and the HOBLink JWT.

#### 6.1.1.2 Information flow control policy model (HTTPS)

The security policy for the HTTPS information flow control policy is defined by the security functional requirements in section 6.1.4. The following is a list of the subjects and resources participating in the policy.

- Subjects:
  - remote trusted entity acting as the client
  - WSP component acting as the server
- Information security attribute:
  - Established TLS connection
- Resources:
  - Protected external web servers;
  - WSP-integrated web server;
- Operation:
  - all data transmissions between the remote trusted entity and the WSP component
- User data:
  - All data transmissions between the remote trusted entity and the WSP component;

#### 6.1.1.3 Information flow control policy model (WSP)

The security policy for the WSP information flow control policy is defined by the security functional requirements in section 6.1.5. The following is a list of the subjects and resources participating in the policy.

- Subject:
  - Authenticated users represented by an HTTP session cookie.  
Note: Within the same browser on the same machine there is only one cookie for an authenticated user that is used for all connection types. This is the HTTP session cookie that is created when the “integrated web server” presents the start web page.
  - Authenticated users represented by an established TLS connection for JWT connections.

- Subject security attributes:
  - Role assigned to the authenticated user of the subject,
  - HTTPS connections: HTTP session cookie,
  - JWT connections: Established TLS connection between HOBLink JWT and the WSP component.
- Resources:
  - Protected Remote Desktop servers;
  - Protected external web servers;
  - WSP-integrated web server.
- TSF data:
  - Configuration information used by the WSP defining the resource access list where access rights are assigned to roles. Therefore, users are also assigned to roles as part of the resource access list.
- User data:
  - All data exchanged between the resources managed by the WSP and the subjects.

## 6.1.2 Cryptographic support

### 6.1.2.1 Cryptographic key generation (FCS\_CKM.1(RNG))

FCS\_CKM.1.1 The TSF shall generate **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **capable of generating a random bit sequence**<sup>7</sup> and specified cryptographic key sizes:

- **AES: 128 bits,**
- **HMAC-SHA1: 160 bits,**
- **HMAC-SHA256: 256 bits**<sup>8</sup>

that meet the following: **cryptographic key generation with random bits generated by:**

- **TLS: generation and exchange of pre-master secrets as defined in the TLSv1.1 protocol [RFC4346] or in the TLSv1.2 protocol [RFC5246] with the cipher suites defined in FCS\_COP.1(TLS)**<sup>9</sup>.

### 6.1.2.2 Cryptographic key generation (FCS\_CKM.1(RSA))

FCS\_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **defined in [FIPS186-3] appendix B.3.3**<sup>10</sup> and specified cryptographic key sizes:

<sup>7</sup> [assignment: cryptographic key generation algorithm]

<sup>8</sup> [assignment: cryptographic key sizes]

<sup>9</sup> [assignment: list of standards]

<sup>10</sup> [assignment: cryptographic key generation algorithm]

- **1536 bits**
- **2048 bits<sup>11</sup>**

that meet the following: **[FIPS186-3]**<sup>12</sup>.

Application Note: The primes used for the RSA key are generated based on random numbers derived out of the RNG specified in FCS\_RNG.1. The TOE uses the Miller-Rabin test to validate that the random values are prime. Therefore, the primes are considered “probable prime”.

Application Note: The prime requirements for the RSA keys are derived from [FIPS186-3] appendix B.3.3 and the minimum number of rounds of M-R testing is determined according to table C.3 in [FIPS186-3]. To define the number of necessary rounds in the Miller-Rabin test for values of prime numbers for RSA key sizes (such as 1536 bits) that are not listed in the table the following methods shall be used. The intermediate value for sizes of prime numbers are determined by the larger number of rounds of the next smaller size of a prime number found in the table. This is equal to the value of rounds for the primes  $p = 512$  and  $q = 512$  in the case of a 1536 bit RSA key. Alternatively the number of rounds for a 1536 bit RSA key may be approximated by a linear interpolation of the requirements for the surrounding key sizes 1024 bits and 2048 bits.

Application Note: The algorithm for the RSA key generation as described in appendix B.3.3 of [FIPS186-3] is not fully congruent with the actual implementation in the source code. The details of the differences are outlined in the TOE design documentation. It is claimed that the parameters created from the implemented RSA key generation will pass all conditions as specified in appendix B.3.3 of [FIPS186-3], except for item 1., which restricts possible key sizes, and the random extraction iteration limit. The TOE design documentation provides the necessary information to prove this claim.

Application Note: The RSA key generation mechanism is used to generate all RSA keys required by the TOE, including root keys, potentially intermediate keys, and leaf keys.

### 6.1.2.3 Cryptographic key distribution (FCS\_CKM.2)

FCS\_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with **a *the following*** specified cryptographic key distribution methods ~~[assignment: cryptographic key distribution method]~~ that meets the following:

- RSA encryption of cryptographic sensitive parameters as defined in [RFC4346] and [RFC5246];**
- Transmission of the client HOBLink Security Unit from the WSP to the “HOBLink Secure, Client” using the established TLS channel specified by the “HOB HTTPS information flow control policy”<sup>13,14</sup>;**
- TLS server certificate distribution as defined in [RFC4346] and [RFC5246].**

Application Note: The TLS channel ends at the client browser whereas the client HOBLink Security Unit is fed into the “HOBLink Secure, Client” by the client browser.

<sup>11</sup> [assignment: cryptographic key sizes]

<sup>12</sup> [assignment: list of standards]

<sup>13</sup> [assignment: cryptographic key distribution method]

<sup>14</sup> [assignment: list of standards]

#### 6.1.2.4 Cryptographic key destruction (FCS\_CKM.4)

FCS\_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **overwriting with zeros**<sup>15</sup> that meets the following: **vendor-specific zeroization**<sup>16</sup>.

Application Note: The "vendor-specific zeroization" covers the following concepts:

- Memory objects: Overwriting the memory with zeros at the time the memory is not further required.

#### 6.1.2.5 Cryptographic operation (FCS\_COP.1(TLS))

FCS\_COP.1.1 The TSF shall perform **encryption, decryption, integrity verification, peer authentication**<sup>17</sup> in accordance with a specified **the following** cryptographic algorithms ~~[assignment: cryptographic algorithm]~~ and, cryptographic key sizes ~~[assignment: cryptographic key sizes]~~ that meet the following: ~~[assignment: list of standards]~~ **and applicable standards:**

a) **TLS version 1.1 defined by [RFC4346] with the following properties:**

- **AES defined in [FIPS197] in CBC mode defined by [SP800-38A] with 128 bits key size,**
- **HMAC defined by [RFC2104],**
- **SHA-1 defined by [FIPS180] used for the pseudo-random function and MAC,**
- **MD5 defined by [RFC1321] used for the pseudo-random function only,**
- **RSA with a key size of either 1536 or 2048 bits;**

b) **TLS version 1.2 defined by [RFC5246] with the following properties:**

- **AES defined in [FIPS197] in CBC mode defined by [SP800-38A] with 128 bits key size,**
- **HMAC defined by [RFC2104],**
- **SHA-1 defined by [FIPS180] used for MAC,**
- **SHA-256 defined by [FIPS180] used for the pseudo-random function and MAC,**
- **RSA with a key size of either 1536 or 2048 bits.**<sup>181920</sup>

Application Note: For TLSv1.1, the following cipher suite is implemented: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA. Any other cipher suite defined in the RFC is not implemented.

<sup>15</sup> [assignment: cryptographic key destruction method]

<sup>16</sup> [assignment: list of standards]

<sup>17</sup> [assignment: list of cryptographic operations]

<sup>18</sup> [assignment: cryptographic algorithm]

<sup>19</sup> [assignment: cryptographic key sizes]

<sup>20</sup> [assignment: list of standards]

Application Note: For TLSv1.2, the following cipher suites are implemented: TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA and TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256. Any other cipher suite defined in the RFC is not implemented.

Application Note: The protocols of TLSv1.1 and TLSv1.2 are implemented with the RSAES-PKCS1-v1\_5 encryption scheme defined in [PKCS1].

#### 6.1.2.6 Cryptographic operation (FCS\_COP.1(CERT))

FCS\_COP.1.1 The TSF shall perform **signature generation and verification**<sup>21</sup> in accordance with a specified **the following** cryptographic algorithms-  
[assignment: cryptographic algorithm] and, cryptographic key sizes  
[assignment: cryptographic key sizes] that meet the following: [assignment: list of standards] **and applicable standards:**

- a) **Signing of an X.509 certificate defined by [RFC5280] using :**
  - o **RSA with key size of either 1536 bits or 2048 bits**
  - o **SHA-1, SHA-256;**
- b) **Verification of an X.509 certificate defined by [RFC5280] using:**
  - o **RSA with key size of either 1536 bits or 2048 bits**
  - o **SHA-1, SHA-256.**<sup>222324</sup>

Application Note: Padding is implemented based on the RSASSA-PKCS1-v1\_5 signature scheme defined in [PKCS1].

#### 6.1.2.7 Random number generation (Class DRG.3) (FCS\_RNG.1)

FCS\_RNG.1.1 The TSF shall provide a deterministic random number generator that implements:

- a) DRG.3.1: If initialized with a random seed **using timing of key strokes by users, timing of movement of mouse by users, variances of CPU load, timing of OS API calls, Linux "/dev/random" output, timing of TCP handshake as random source**<sup>25</sup>, the internal state of the RNG shall **have a Min-entropy**<sup>26</sup> **of 48 bits**<sup>27</sup>.
- b) DRG.3.2: The DRNG provides forward secrecy.
- c) DRG.3.3: The DRNG provides backward secrecy even if the current internal state is known.

FCS\_RNG.1.2 The TSF shall provide random numbers that meet:

<sup>21</sup> [assignment: list of cryptographic operations]

<sup>22</sup> [assignment: cryptographic algorithm]

<sup>23</sup> [assignment: cryptographic key sizes]

<sup>24</sup> [assignment: list of standards]

<sup>25</sup> [selection: using PTRNG of class PTG.2 as random source, using PTRNG of class PTG.3 as random source, using NPTRNG of class NTG.1 as random source, [assignment: other requirements for seeding]]

<sup>26</sup> defined in [KS2011]

<sup>27</sup> [selection: have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]]

- a) DRG.3.4: The RNG initialized with a random seed **at initialization time of the DRNG**<sup>28</sup> generates output for which  **$2^{32}$** <sup>29</sup> strings of bit length 128 are mutually different with probability **of greater than  $1-2^{-10}$** <sup>30</sup>.
- b) DRG.3.5: Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A<sup>31</sup>.

Application Note: The TOE implements the CTR\_DRBG with AES 128 core according to the specification of NIST SP800-90A.

Application Note: The TOE implements the specified RNG in the following components:

- the WSP implements one RNG for handling the TLS connections and the HTTP session cookie generation,
- the HOBLink Security Manager implements the RNG to support the key and certificate generation, and
- the HOBLink JWT implementing one RNG for handling the TLS connections.

Application Note: The TOE implements the specified RNG which uses the following random sources in the following components:

- the WSP initializes the RNG using variances of CPU load, timing of OS API calls, Linux "/dev/random" output and timing of TCP handshake,
- the HOBLink Security Manager initializes the RNG using timing of key strokes by users and timing of movement of mouse by users, and
- the HOBLink JWT initializes the RNG using timing of key strokes by users and timing of movement of mouse by users.

### 6.1.3 JWT TLS connectivity

#### 6.1.3.1 Subset information flow control (FDP\_IFC.1(JWT))

FDP\_IFC.1.1 The TSF shall enforce the **JWT TLS information flow control policy**<sup>32</sup> on

- **Subjects:**
  - **HOBLink JWT component acting as the client**
  - **WSP component acting as the server**
- **Information:**
  - **all encapsulated RDP user data,**
  - **X.509 certificate**
- **Operation:**

<sup>28</sup> [assignment: requirements for seeding]

<sup>29</sup> [assignment: number of strings]

<sup>30</sup> [assignment: probability]

<sup>31</sup> [assignment: additional test suites]

<sup>32</sup> [assignment: information flow control SFP]

- **all data transmissions between the HOBLink JWT component and the WSP component<sup>33</sup>.**

### 6.1.3.2 Simple security attributes (FDP\_IFF.1(JWT))

FDP\_IFF.1.1 The TSF shall enforce the **JWT TLS information flow control policy<sup>34</sup>** based on the following types of subject and information security attributes:

- **Information security attributes:**
  - **RDP user data: Established TLS connection,**
  - **For each X.509 certificate:**
    - **Digital signature generated with the X.509 certificate,**
    - **Distinguished Name (DN) stored in an X.509 certificate,**
    - **Validity period of X.509 certificate,**
    - **BasicConstraints<sup>35</sup>.**

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:

- **“HOBLink Secure, Server” within the WSP component presents an X.509v3 certificate according to [RFC5280] to “HOBLink Secure, Client” within the HOBLink JWT component and “HOBLink Secure, Client” within the HOBLink JWT supported by HOBLink JWT performs the following validity checks:**
  1. **For server certificate:**
    - **Validity of digital signature of X.509 certificate presented by peer,**
    - **Validity period of X.509 certificate started and did not end,**
    - **The Common Name part of the Distinguished Name component stored in the X.509 certificate matches either:**
      - **the IP address of the WSP server, or**
      - **the DNS name of the WSP server;**
  2. **Certificate chain validation: If current certificate is not the root certificate known to the validation mechanism, the following checks are performed for each certificate of the certificate chain that signed the current server certificate and all intermediate certificates:**

<sup>33</sup> [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]

<sup>34</sup> [assignment: information flow control SFP]

<sup>35</sup> [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]

- **Validity of digital signature of signed X.509 certificate,**
  - **Validity period of X.509 certificate started and did not end,**
  - **BasicConstraints mark the certificate as a CA or sub-CA certificate,**
  - **Root certificate is self signed and is already known to the validation mechanism, and**
  - **Chain of certificate signatures leading from the root certificate to the server certificate is complete.**
- **“HOBLink Secure, Server” within the WSP component and “HOBLink Secure, Client” within the HOBLink JWT component ensure that a communication link using either of the following protocols is successfully established:**
    - **TLS version 1.1**
    - **TLS version 1.2<sup>36</sup>.**

FDP\_IFF.1.3 The TSF shall enforce the **no other information flow control SFP rules<sup>37</sup>.**

FDP\_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **none<sup>38</sup>.**

FDP\_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **none<sup>39</sup>.**

### 6.1.3.3 Basic internal transfer protection (FDP\_ITT.1)

FDP\_ITT.1.1 The TSF shall enforce the **JWT TLS information flow control policy<sup>40</sup>** to prevent the **disclosure, modification<sup>41</sup>** of user data when it is transmitted between physically-separated parts of the TOE.

### 6.1.3.4 Integrity monitoring (FDP\_ITT.3)

FDP\_ITT.3.1 The TSF shall enforce the **JWT TLS information flow control policy<sup>42</sup>** to monitor user data transmitted between physically-separated parts of the TOE for the following errors:

- **modification of data,**
- **reordering of data,**
- **deletion of data,**
- **insertion of data,**

<sup>36</sup> [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]

<sup>37</sup> [assignment: additional information flow control SFP rules]

<sup>38</sup> [assignment: rules, based on security attributes, that explicitly authorise information flows]

<sup>39</sup> [assignment: rules, based on security attributes, that explicitly deny information flows]

<sup>40</sup> [assignment: access control SFP(s) and/or information flow control SFP(s)]

<sup>41</sup> [selection: disclosure, modification, loss of use]

<sup>42</sup> [assignment: access control SFP(s) and/or information flow control SFP(s)]



- **replay of data**<sup>43</sup>.

FDP\_ITT.3.2 Upon detection of a data integrity error, the TSF shall **terminate the TLS session and inform the application about the reason of the termination**<sup>44</sup>.

#### 6.1.3.5 Configuration value initialization (FMT\_CFG.2(JWT))

FMT\_CFG.2.1 The TSF shall enforce the **JWT TLS information flow control policy**<sup>45</sup> to provide **restrictive**<sup>46</sup> default values for security attributes that are used to enforce the SFP.

FMT\_CFG.2.2 The TSF shall support the specification of alternative initial values to override the default values used in enforcing the security policy.

### 6.1.4 HTTPS connectivity

#### 6.1.4.1 Subset information flow control (FDP\_IFC.1(HTTPS))

FDP\_IFC.1.1 The TSF shall enforce the **HOB HTTPS information flow control policy**<sup>47</sup> on

- **Subjects:**
  - **remote trusted entity acting as the client**
  - **WSP component acting as the server**
- **Information:**
  - **all encapsulated web user data,**
  - **HOBLink JWT webstart application and client HOBLink Security Unit**
- **Operation:**
  - **all data transmissions between the remote trusted entity and the WSP component**<sup>48</sup>.

#### 6.1.4.2 Simple security attributes (FDP\_IFF.1(HTTPS))

FDP\_IFF.1.1 The TSF shall enforce the **HOB HTTPS information flow control policy**<sup>49</sup> based on the following types of subject and information security attributes:

- **Information security attribute:**
  - **Established TLS connection**<sup>50</sup>.

<sup>43</sup> [assignment: integrity errors]

<sup>44</sup> [assignment: specify the action to be taken upon integrity error]

<sup>45</sup> [assignment: access control SFP, information flow control SFP]

<sup>46</sup> [selection, choose one of: restrictive, permissive, [assignment: other property]]

<sup>47</sup> [assignment: information flow control SFP]

<sup>48</sup> [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]

<sup>49</sup> [assignment: information flow control SFP]

<sup>50</sup> [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]

- 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:
- **“HOBLink Secure, Server” within the WSP component ensures that a communication link using either of the following protocols is successfully established:**
    - **TLS version 1.1**
    - **TLS version 1.2<sup>51</sup>.**
- FDP\_IFF.1.3 The TSF shall enforce the **no other information flow control SFP rules<sup>52</sup>.**
- FDP\_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **none<sup>53</sup>.**
- FDP\_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **none<sup>54</sup>.**

#### 6.1.4.3 Configuration value initialization (FMT\_CFG.2(HTTPS))

- FMT\_CFG.2.1 The TSF shall enforce the **HOB HTTPS information flow control policy<sup>55</sup>** to provide **restrictive<sup>56</sup>** default values for security attributes that are used to enforce the SFP.
- FMT\_CFG.2.2 The TSF shall support the specification of alternative initial values to override the default values used in enforcing the security policy.

#### 6.1.4.4 Inter-TSF trusted channel (FTP\_ITC.1)

- FTP\_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification ~~or~~ **and disclosure using the following mechanisms: Cryptographically-protected communication channel using:**
- **TLS v1.1, or**
  - **TLS v1.2.**
- FTP\_ITC.1.2 The TSF shall permit **another trusted IT product<sup>57</sup>** to initiate communication via the trusted channel.
- FTP\_ITC.1.3 The TSF shall initiate communication via the trusted channel for **communication with the external entity<sup>58</sup>.**

Application Note: The SFR applies to the communication between the client Browser and the WSP.

<sup>51</sup> [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]

<sup>52</sup> [assignment: additional information flow control SFP rules]

<sup>53</sup> [assignment: rules, based on security attributes, that explicitly authorise information flows]

<sup>54</sup> [assignment: rules, based on security attributes, that explicitly deny information flows]

<sup>55</sup> [assignment: access control SFP, information flow control SFP]

<sup>56</sup> [selection, choose one of: restrictive, permissive, [assignment: other property]]

<sup>57</sup> [selection: the TSF, another trusted IT product]

<sup>58</sup> [assignment: list of functions for which a trusted channel is required]

## 6.1.5 Identification, Authentication and Authorization

### 6.1.5.1 Complete information flow control (FDP\_IFC.2)

FDP\_IFC.2.1 The TSF shall enforce the **WSP information flow control policy**<sup>59</sup> on

- **Subjects:**
  - **HTTPS connections: Authenticated users represented by the HTTP session cookie;**
  - **JWT connections: Authenticated users represented by an established TLS connection;**
- **Information**
  - **All data flowing between subjects and resources of web servers and Remote Desktop servers protected by the WSP;**<sup>60</sup>

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP\_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

### 6.1.5.2 Simple security attributes (FDP\_IFF.1(WSP))

FDP\_IFF.1.1 The TSF shall enforce the **WSP information flow control policy**<sup>61</sup> based on the following types of subject and information security attributes:

- **Subject security attributes:**
  - **Role assigned to the authenticated user of the subject,**
  - **HTTPS connections: HTTP session cookie,**
  - **JWT connections: Established TLS connection between HOBLink JWT and the WSP component**<sup>62</sup>.

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: **the subject's information flow to the protected resources of web servers or Remote Desktop servers is allowed if**

- **subject presents either:**
  - **ticket and user information encode in an HTTP session cookie,**
  - **or submits the data via an established TLS connection between HOBLink JWT and the WSP component**

<sup>59</sup> [assignment: information flow control SFP]

<sup>60</sup> [assignment: list of subjects and information]

<sup>61</sup> [assignment: information flow control SFP]

<sup>62</sup> [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]

**that allows the WSP to verify that the request is part of an active session, and**

- **the accessed resource is listed in the access lists assigned to the role the user represented the active session is mapped to<sup>63</sup>.**

FDP\_IFF.1.3 The TSF shall enforce the **no other information flow control SFP rules<sup>64</sup>.**

FDP\_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: **none<sup>65</sup>.**

FDP\_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: **none<sup>66</sup>.**

Application Note: After successful I&A, the state of a connection is maintained as follows:

- As HTTP is a stateless protocol, the state is maintained by the HTTP session cookie and the user must always transmit the HTTP session cookie with each request to map the request to the initially identified user;
- The connection between WSP and JWT is a stateful TLS channel where each request submitted via this established TLS channel is implicitly assigned to the initially identified user.

#### **6.1.5.3 User attribute definition (FIA\_ATD.1)**

FIA\_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **zero or more ephemeral HTTP session cookies;**
- **zero or more ephemeral network connection from the HOBLink JWT component<sup>67</sup>.**

Application Note: The identification and authentication is performed by requiring a username/password combination to be entered by the user. These credentials are used to perform an LDAP-bind operation to verify these credentials. Since the LDAP server performs the identification/authentication decision and the TOE enforces this decision, the TOE does not maintain or require any of the credentials.

#### **6.1.5.4 Timing of authentication (FIA\_UAU.1)**

FIA\_UAU.1.1 The TSF shall allow

- **initiation of the TLS connection tunneling the HTTP requests,**
- **access to the logon web page offered by the WSP<sup>68</sup>**

on behalf of the user to be performed before the user is authenticated.

FIA\_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

<sup>63</sup> [assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]

<sup>64</sup> [assignment: additional information flow control SFP rules]

<sup>65</sup> [assignment: rules, based on security attributes, that explicitly authorise information flows]

<sup>66</sup> [assignment: rules, based on security attributes, that explicitly deny information flows]

<sup>67</sup> [assignment: list of security attributes]

<sup>68</sup> [assignment: list of TSF mediated actions]

**6.1.5.5 Timing of identification (FIA\_UID.1)**

FIA\_UID.1.1 The TSF shall allow

- **initiation of the TLS connection tunneling the HTTP requests,**
- **access to the logon web page offered by the WSP<sup>69</sup>**

on behalf of the user to be performed before the user is identified.

FIA\_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

**6.1.5.6 User-subject binding (FIA\_USB.1)**

FIA\_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

- **HTTPS connection: HTTP session cookie,**
- **JWT connection:**
  - **HTTP session cookie for the authentication after the establishment of the JWT TLS connection, and**
  - **an established TLS connection<sup>70</sup>.**

FIA\_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users:

- **HTTPS connection: Upon successful identification and authentication, WSP issues a unique HTTP session cookie which the WSP relates to the current HTTPS connection;**
- **JWT connection: The establishment of a JWS connection requires a valid and established HTTPS connection where the JWS connection re-uses and re-submits the existing HTTP session cookie which the WSP relates to newly initiated JWT connection<sup>71</sup>.**

FIA\_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **none<sup>72</sup>.**

**6.1.5.7 Configuration value initialization (FMT\_CFG.2(WSP))**

FMT\_CFG.2.1 The TSF shall enforce the **WSP information flow control policy<sup>73</sup>** to provide **restrictive<sup>74</sup>** default values for security attributes that are used to enforce the SFP.

FMT\_CFG.2.2 The TSF shall support the specification of alternative initial values to override the default values used in enforcing the security policy.

<sup>69</sup> [assignment: list of TSF mediated actions]

<sup>70</sup> [assignment: list of user security attributes]

<sup>71</sup> [assignment: rules for the initial association of attributes]

<sup>72</sup> [assignment: rules for the changing of attributes]

<sup>73</sup> [assignment: access control SFP, information flow control SFP]

<sup>74</sup> [selection, choose one of: restrictive, permissive, [assignment: other property]]

Application Note: The restrictive default values apply to the allowed information flow: if the administrator did not specify any information flow rules, no connection is allowed by the WSP. Only when rules are specified, WSP allows communication based on those rules and denies any other traffic.

### 6.1.5.8 Configuration of security functions (FMT\_CFG.1)

FMT\_CFG.1.1 The TSF shall be capable of configuring the following security functions: **access control via access lists specifying the allowed resources protected by the WSP holding the following information:**

- **access control rules mapping resources to roles,**
- **role specifications mapping users to roles<sup>75</sup>.**

## 6.2 Security Functional Requirements Rationale

### 6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Table 19: Mapping of security functional requirements to security objectives

Security Functional Requirements	Objectives
FCS_CKM.1(RNG)	O.Crypto.Net
FCS_CKM.1(RSA)	O.Certificates
FCS_CKM.2	O.Crypto.Net
FCS_CKM.4	O.Crypto.Net, O.Certificates
FCS_COP.1(TLS)	O.Crypto.Net
FCS_COP.1(CERT)	O.Certificates, O.CryptoNet
FCS_RNG.1	O.Crypto.Net, O.Certificates, O.I&A
FDP_IFC.1(JWT)	O.Crypto.Net
FDP_IFF.1(JWT)	O.Crypto.Net
FDP_ITT.1	O.Crypto.Net
FDP_ITT.3	O.Crypto.Net
FMT_CFG.2(JWT)	O.Crypto.Net
FDP_IFC.1(HTTPS)	O.Crypto.Net
FDP_IFF.1(HTTPS)	O.Crypto.Net
FMT_CFG.2(HTTPS)	O.Crypto.Net
FTP_ITC.1	O.CryptoNet
FDP_IFC.2	O.Resource.Access

<sup>75</sup> [assignment: list of functions to be configurable by the TSF]

Security Functional Requirements	Objectives
FDP_IFF.1(WSP)	O.Resource.Access
FIA_ATD.1	O.I&A
FIA_UAU.1	O.I&A
FIA_UID.1	O.I&A
FIA_USB.1	O.I&A
FMT_CFG.2(WSP)	O.Resource.Access
FMT_CFG.1	O.Resource.Access

### 6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Table 20: Security objectives for the TOE rationale

Security objectives	Rationale
O.Certificates	<p>The objective that the TOE provides the facility to generate RSA certificates and the corresponding keys is implemented with:</p> <ul style="list-style-type: none"> <li>• FCS_CKM.1(RSA) defining the RSA key generation mechanism and creating X.509 certificates from the RSA keys (FCS_COP.1(CERT)).</li> <li>• FCS_CKM.4 which zeroizes the memory used for RSA keys.</li> <li>• FCS_RNG.1 supporting the key generation by providing random numbers.</li> </ul>
O.Crypto.Net	<p>The objective that the TSF must be designed and implemented in a manner that allows for establishing a trusted channel between the TOE and a remote trusted IT system that protects the user data and TSF data transferred over this channel from disclosure and undetected modification and prevents masquerading of the remote trusted IT system is implemented with:</p> <ul style="list-style-type: none"> <li>• Providing cryptographic primitives for key generation (FCS_CKM.1(RNG)) supported by a deterministic RNG as defined in FCS_RNG.1;</li> <li>• Providing the cryptographic protocol of TLS including the key and certificate exchange mechanism (FCS_CKM.2, FCS_COP.1(TLS), FCS_COP.1(CERT));</li> <li>• Zeroization of key material and other ephemeral cryptographic sensitive data (FCS_CKM.4);</li> <li>• Use and definition of properties of the TLS channel with uni-directional certificate validation used by the HOBLINK JWT component connecting to the WSP component (FDP_IFC.1(JWT), FDP_IFF.1(JWT), FDP_ITT.1, FDP_ITT.3, FMT_CFG.2(JWT));</li> <li>• Use and definition of properties of the TLS channel used by the environmental web browser connecting to the WSP component (FDP_IFC.1(HTTPS), FDP_IFF.1(HTTPS), FMT_CFG.2(HTTPS), FTP_ITC.1).</li> </ul>

Security objectives	Rationale
O.I&A	<p>The objective that the TOE must ensure that users have been successfully authenticated before allowing any action the TOE has defined to provide to authenticated users only is implemented with:</p> <ul style="list-style-type: none"> <li>• Generation of the HTTPS session cookie (FCS_RNG.1);</li> <li>• Maintenance of ephemeral user data (FIA_ATD.1);</li> <li>• Specification of the identification and authentication method (FIA_UAU.1, FIA_UID.1);</li> <li>• Definition of the user-subject binding mechanism (FIA_USB.1).</li> </ul>
O.Resource. Access	<p>The objective that the TSF must control access of subjects and/or users to the resources of web servers and Remote Desktop servers based on identity of the resource is implemented by:</p> <ul style="list-style-type: none"> <li>• The information flow control policy that governs the access of subjects to resources (FDP_IFC.2, FDP_IFF.1(WSP), FMT_CFG.2(WSP));</li> <li>• Management interface for the information flow control policy (FMT_CFG.1).</li> </ul>

### 6.2.3 Security requirements dependency analysis

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Table 21: TOE SFR dependency analysis

Security Functional Requirements	Dependencies	Resolution
FCS_CKM.1(RNG)	[FCS_CKM.2 or FCS_COP.1]	Yes: FCS_CKM.2, FCS_COP.1(TLS)
	FCS_CKM.4	Yes: FCS_CKM.4
FCS_CKM.1(RSA)	[FCS_CKM.2 or FCS_COP.1]	Yes: FCS_CKM.2, FCS_COP.1
	FCS_CKM.4	Yes: FCS_CKM.4, covering the copies of the RSA keys in memory.
		Uncovered: FCS_CKM.4 – The objective for the environment OE.DestroyRSA ensures that environmental procedures are in place that ensure the destruction of long-lived RSA keys.
		Uncovered: FCS_CKM.2 for the distribution of keys between the HOBLink Security Manager and the WSP which is covered by OE.SecMgr.



Security Functional Requirements	Dependencies	Resolution
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes: FCS_CKM.1(RNG) and FCS_CKM.1(RSA)
	FCS_CKM.4	Yes: FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes: FCS_CKM.1(RNG), FCS_CKM.1(RSA)
FCS_COP.1(TLS)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes: FCS_CKM.1(RNG) and FCS_CKM.1(RSA)
	FCS_CKM.4	Yes: FCS_CKM.4
FCS_COP.1(CERT)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Yes: FCS_CKM.1(RSA)
	FCS_CKM.4	Yes: FCS_CKM.4
FCS_RNG.1	No dependencies	Yes
FDP_IFC.1(JWT)	FDP_IFF.1	Yes: FDP_IFF.1(JWT)
FDP_IFF.1(JWT)	FDP_IFC.1	Yes: FDP_IFC.1(JWT)
	FDP_MSA.3	NO: The TOE does not support administrative roles. Therefore the configuration aspects are covered by FMT_CFG.2(JWT) instead of FMT_MSA.3.
FDP_ITT.1	[FDP_ACC.1 or FDP_IFC.1]	Yes: FDP_IFC.1(JWT)
FDP_ITT.3	[FDP_ACC.1 or FDP_IFC.1]	Yes: FDP_IFC.1(JWT)
	FDP_ITT.1	Yes: FDP_ITT.1
FMT_CFG.2(JWT)	No dependencies	Yes
FDP_IFC.1(HTTPS)	FDP_IFF.1	Yes: FDP_IFF.1(HTTPS)
FDP_IFF.1(HTTPS)	FDP_IFC.1	Yes: FDP_IFC.1(HTTPS)
	FDP_MSA.3	NO: The TOE does not support administrative roles. Therefore the configuration aspects are covered by FMT_CFG.2(HTTPS) instead of FMT_MSA.3.
FMT_CFG.2(HTTPS)	No dependencies	Yes
FTP_ITC.1	No dependencies	Yes.

<b>Security Functional Requirements</b>	<b>Dependencies</b>	<b>Resolution</b>
FDP_IFC.2	FDP_IFF.1	Yes: FDP_IFF.1(WSP)
FDP_IFF.1(WSP)	FDP_IFC.1	Yes: FDP_IFC.2
	FDP_MSA.3	Yes: FMT_CFG.2(WSP)
FIA_ATD.1	No dependencies	Yes
FIA_UAU.1	FIA_UID.1	Yes: FIA_UID.1
FIA_UID.1	No dependencies	
FIA_USB.1	FIA_ATD.1	Yes: FIA_ATD.1
FMT_CFG.2(WSP)	No dependencies	Yes
FMT_CFG.1	No dependencies	Yes

### 6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the EAL4 components as specified in [CC] part 3, augmented by ALC\_FLR.2.

The following table shows the Security assurance requirements, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Table 22: Security assurance requirements

<b>Security assurance class</b>	<b>Security assurance requirement</b>	<b>Source</b>	<b>Operations</b>			
			<b>Iter.</b>	<b>Ref.</b>	<b>Ass.</b>	<b>Sel.</b>
ADV	ADV_ARC.1	CC Part 3				
	ADV_FSP.4	CC Part 3				
	ADV_IMP.1	CC Part 3				
	ADV_TDS.3	CC Part 3				
AGD	AGD_OPE.1	CC Part 3				
	AGD_PRE.1	CC Part 3				
ALC	ALC_CMC.4	CC Part 3				
	ALC_CMS.4	CC Part 3				
	ALC_DEL.1	CC Part 3				
	ALC_DVS.1	CC Part 3				
	ALC_FLR.2	CC Part 3				
	ALC_LCD.1	CC Part 3				
	ALC_TAT.1	CC Part 3				

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ASE	ASE_INT.1	CC Part 3				
	ASE_CCL.1	CC Part 3				
	ASE_SPD.1	CC Part 3				
	ASE_OBJ.2	CC Part 3				
	ASE_ECD.1	CC Part 3				
	ASE_REQ.2	CC Part 3				
	ASE_TSS.1	CC Part 3				
ATE	ATE_COV.2	CC Part 3				
	ATE_DPT.1	CC Part 3				
	ATE_FUN.1	CC Part 3				
	ATE_IND.2	CC Part 3				
AVA	AVA_VAN.3	CC Part 3				

## 6.4 Security Assurance Requirements Rationale

The basis for the justification of EAL4 is the threat environment experienced by the typical consumers of the TOE. This matches the package description for EAL4.

In addition, the evaluation assurance level has been augmented with ALC\_FLR.2 commensurate with the flaw remediation capabilities offered by the developer beyond those required by the evaluation assurance level.

## 7 TOE Summary Specification

### 7.1 TOE Security Functionality

The following section explains how the security functions are implemented. The different TOE security functions cover the various SFR classes.

The primary security features of the TOE are:

- Cryptographic primitives
- Certificate generation
- Establishment and maintenance of TLS protected links
- Identification, authentication and authorization

### 7.1.1 Cryptographic primitives

The TOE implements the TLSv1.1 as well as TLSv1.2 protocols as specified in the respective RFC. The product does not use third party classes to provide this functionality. All cryptographic primitives required by the protocols as well as other services in the TOE are fully implemented in the TOE, including:

- generation of symmetric keys, including cryptographic sensitive parameters for HMACs, the TLS handshake (such as pre-master secret), padding for RSA and the generation of HTTP session cookies;
- verification of RSA keys and certificates;
- deterministic random number generator seeded by noise sources developed by HOB and operational on all underlying systems allowed by this ST.

The “HOBLink Secure, Client” module within the HOBLink JWT component reflects the “client” as specified in TLS and the HOB WebSecureProxy (WSP) component that includes the “HOBLink Secure, Server” module implements the “server” as specified in TLS.

Any key material and cryptographically sensitive parameters are zeroized after use.

This functionality covers the SFRs of: FCS\_CKM.1(RNG), FCS\_CKM.4, FCS\_COP.1(CERT), FCS\_RNG.1.

#### 7.1.1.1 General characteristics of the TLS protocol

The first phase within the TLS protocol is the handshake protocol, in which a cryptographic cipher suite (consisting of an asymmetric algorithm, a bulk data encryption algorithm, the key size for the bulk data encryption algorithm, a hash algorithm) and cryptographic keys (encryption/decryption keys, MAC secrets) are negotiated. Separate bulk data encryption keys and MAC secrets are generated for each communication direction. The handshake protocol uses MD5 and SHA-1 (TLSv1.1) and SHA-256 (TLSv1.2) to create these session keys and MAC secrets. The MAC secrets are used for protecting integrity of the information exchanged.

After the handshake protocol has been successfully completed, user data can be securely transferred according to the agreed cipher suite. The TLS protocol ensures the confidentiality and integrity of transmitted user data.

Integrity is achieved specifically by the HMAC mechanism for message authentication using cryptographic hash functions in combination with the secret shared keys (MAC secrets).

Concealment of asymmetric encrypted secrets is achieved by adding random padding bytes. A proper implementation of the TLS protocol allows detection of modification of data, substitution of data, re-ordering of data, deletion of data, insertion of data, replay of data and prevents disclosure of data.

This functionality covers the SFRs of: FCS\_COP.1(TLS).

#### 7.1.1.2 TLS implementation in the TOE

In the course of the handling of the TLS handshake protocol, the “HOBLink Secure, Client” module within HOBLink JWT and the “HOBLink Secure, Server” module within the WSP negotiate on (TLSv1.1: RSA, AES 128 bits, TLSv1.2: RSA, AES 128 bits) as the cipher suite. These modules generate a TLS master secret out of the pre-master secret protected using RSA encryption of 48 Bytes length from which keys used for AES and for MAC secrets using

HMAC-SHA-1 or HMAC-SHA-256, respectively. User data is transferred only after a TLS handshake has been successfully completed.

For the HTTPS connections, the TOE does not perform any certificate validation. The WSP sends its server certificate to the web browser. The web browser together with the user is assumed to correctly verify the WSP server certificate to prevent any man-in-the-middle attacks and any derived attacks.

For the JWT connection, WSP again offers its server certificate to the HOBLink JWT component. The HOBLink Client Security Unit holds all certificates needed for key chain validation. Using the downloaded HOBLink Client Security Unit HOBLink JWT performs the certificate verification, including the certificate chain validation.

This functionality covers the SFRs of: FCS\_CKM.2, FCS\_COP.1(CERT), FCS\_COP.1(TLS).

### 7.1.2 Certificate Generation

The Security Manager component is able to generate RSA keys and issue X.509v3 certificates for these keys according to [RFC5280] with digital signatures based on the properties documented in FCS\_COP.1(CERT). In the evaluated configuration the Security Manager generates RSA keys with a modulus size of 1536 bits or 2048 bits that are constructed from random numbers proven to be prime. The implemented cryptographic key generation algorithm is a slightly modified version of the algorithm defined in [FIPS186-3] appendix B.3.3. Primality of the numbers used to create a RSA modulus is tested using the Miller-Rabin test. The Miller-Rabin algorithm is implemented according to section C.3.1 of [FIPS186-3] which equals the description of D.E. Knuth in [KNUT\_CPRG\_II] (Factoring into primes, Algorithm P). It is also described in [ISO\_IEC\_18032] and [X9.31], and table C.3 of [FIPS186-3] determines the test requirements, (also found in Annex A.3, table A.1 in [ISO\_IEC\_18032]). [HboAppCryp] is used to verify the implemented algorithms against a further source of information (p.139, p.165).

The RNG used for the generation of the RSA components is the Java implementation of the same RNG algorithm used for the WSP.

This functionality covers the SFRs of: FCS\_CKM.1(RSA), FCS\_COP.1(CERT), FCS\_RNG.1.

### 7.1.3 Establishment and maintenance of TLS protected links

The TOE requires that the client web browser initiates an HTTPS session based on TLSv1.1 or TLSv1.2 with the WSP component before any additional operation can proceed. If the web browser fails to use the mentioned cryptographic protocols, WSP will terminate the connection.

WSP also enforces the continued use of the HTTPS connection with the validation of the HTTP session cookie (related to the user) when accessing protected web servers for each access request. WSP decrypts the HTTPS requests and forwards these as HTTP requests to the intended web server.

To initiate a session with a protected Remote Desktop server, the client web browser together with its JVM is instructed to download the HOBLink JWT Java Webstart application using an HTTPS connection to the given destination address (of the WSP) while presenting the HTTPS session cookie. The HOBLink JWT Java Webstart application is started using the parameters given in the HOBLink JWT Java Webstart file presented at the link of the Remote Desktop server. The HOBLink JWT Java Webstart file contains all necessary parameters. WSP now waits for a new TLS session to be initiated by HOBLink JWT. The HOBLink JWT application initiates the TLS handshake and performs the server certificate verification with the rules as defined in FDP\_IFF.1(JWT) and assures that any subsequent

RDP data exchanged with the accessed Remote Desktop server is routed through the newly instantiated TLS link.

A TLS channel is established after all certificate validation passed successfully. Without a HOBLink Client Security Unit, a TLS channel cannot be established.

This functionality covers the SFRs of:

- JWT: FDP\_IFC.1(JWT), FDP\_IFF.1(JWT), FDP\_ITT.1, FDP\_ITT.3, FMT\_CFG.2(JWT);
- HTTPS: FDP\_IFC.1(HTTPS), FDP\_IFF.1(HTTPS), FMT\_CFG.2(HTTPS), FTP\_ITC.1.

#### **7.1.4 Identification, authentication and authorization**

WSP implements a gateway to the protected resources of web servers and Remote Desktop servers. Before users are allowed to connect to these servers, WSP requires the user to supply a username and password. These credentials are used to perform an LDAP-bind operation to verify these credentials. If the LDAP server rejects the LDAP-bind operation with these credentials, WSP also rejects the user. Otherwise the user is identified and authenticated.

If the user is successfully identified and authenticated, the WSP retrieves the JWT and WSG configuration for the logged-in user. In the next step the integrated web server in the HTTP Handler module within the WSP generates a start web page for the logged-in user. The start web page includes the links to the protected destination servers that the user is allowed to access. Every link leads to one accessible server either with HOBLink JWT for an RDP session or with the browser for web servers. The list of links to web servers is determined by the user's configuration, but can be restricted by target filter entries in the WSP configuration file. The WSP configuration file that is stored in a folder of the RD VPN installation is configured by an authorized administrator.

A user now can access the destination servers via the links on the start web page. All authorization relevant constraints that are active for access security are performed by the WSP and determined in the WSP configuration based on role-based access control rules specified in an access control list. Any communication established by selecting these URLs always implies that the WSP is used as a gateway. Thus, the WSP is able to enforce the configured authorization based on:

- the HTTP session cookies to be delivered by the client web browser with each HTTPS request;
- the HTTP session cookies to be delivered by HOBLink JWT in a TLS connection that subsequently is used for transporting RDP data of one Remote Desktop session to one Remote Desktop server and back.

The administrator is able to configure the access control list to specify which role is granted access to what resource. Moreover, the assignment of users to roles can be configured by administrators as well.

This functionality covers the SFRs of: FDP\_IFC.2, FDP\_IFF.1(WSP), FIA\_ATD.1, FIA\_UAU.1, FIA\_UID.1, FIA\_USB.1, FMT\_CFG.2(WSP), FMT\_CFG.1.

##### **7.1.4.1 HTTP session cookies**

After the user is identified and authenticated, the HTTP handler within the WSP issues an HTTP session cookie. The web browser must submit this cookie with each HTTPS request.

The WSP uses the cookie to accept further connections initiated and established by the user or, by the user's activities, to prevent repetitive re-authentication by the user.

If a client does not submit a valid HTTP cookie, the request is denied.

HOBLink JWT receives all necessary parameters from the Webstart file the web start page links to when it starts. The HOBLink JWT component submits information of the HTTP session cookie after the successful establishment of the TLS connection to allow WSP to link the new TLS connection with the already authenticated user. The WSP forwards the connection data to the selected Remote Desktop server.

This functionality covers the SFRs of: FCS\_RNG.1, FIA\_ATD.1, FIA\_USB.1.

This page was intentionally left blank.



## 8 Conventions, Terminology, and Acronyms

This section identifies the formatting conventions used to convey additional information, specific terminology and acronyms used throughout the remainder of the document.

### 8.1 Terminology

Application	Connectivity software product, more specifically either HOBLink JWT (RDP connection) or a Web Browser (HTTP connection) that transfers user data between one computer (Client) and another (Server).
Attacker	An unauthorized user who attempts to violate the TSP.
Remote Desktop Server	A software product for servers that allow multiple users to log on simultaneously to a server system that provides sessions for remote desktop clients, sharing the hardware and software resources of the server.
TLS	A common denominator for the TLS protocol 1.1 and 1.2 as specified in [TLS] (for example Microsoft Windows Remote Desktop Session Host).
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User Data	Data created by and for the user, that does not affect the operation of the TSF. User data which is transferred over physically separated parts of the TOE according to the TSP is referred to as “transmitted information”.
TOE Security Policy	A set of rules that regulate how assets are managed, protected and distributed within a TOE.
Web Browser	Software product for Users that requests data from Web Servers using HTTP or HTTPS and displays the information with a GUI.
Web Server	Software product for servers that sends files via HTTP or HTTPS based on requests sent by Web Browsers.

## 9 Index of Tables and Illustrations

### Tables and Illustrations

Table 1: Hardware and Software requirements.....	8
Table 2: JVMs that are currently used for the HOBLink Security Manager.....	8
Table 3: JVMs allowed to be used with HOBLink JWT.....	9
Fig. 1: Overview of HOB RD VPN scenario.....	11
Table 4: Software components of the TOE.....	14
Table 5: Threats to be countered by the TOE.....	18
Table 6: Assumptions to be covered by physical constraints.....	18
Table 7: Assumptions to be covered by personnel constraints.....	18
Table 8: Assumptions to be covered by procedural constraints.....	19
Table 9: Assumptions to be covered by connectivity constraints.....	19
Table 10: Organizational Security Policies to be met by the TOE.....	20
Table 11: Security Objectives for the TOE.....	20
Table 12: Security Objectives for the TOE environment.....	21
Table 13: Mapping of security objectives to threats and policies.....	22
Table 14: Mapping of security objectives for the Operational Environment to assumptions, threats and policies.....	23
Table 15: Sufficiency of objectives countering threats.....	23
Table 16: Sufficiency of objectives holding assumptions.....	24
Table 17: Sufficiency of objectives enforcing Organizational Security Policies.....	27
Table 18: Security functional requirements for the TOE.....	29
Table 19: Mapping of security functional requirements to security objectives.....	44
Table 20: Security objectives for the TOE rationale.....	45
Table 21: TOE SFR dependency analysis.....	46
Table 22: Security assurance requirements.....	48

## 10 Related standards and documents

- [BASE64] RFC 1521: Mechanisms for Specifying and Describing the Format of Internet Message Bodies, September 1993
- [CC] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012, Parts 1 through 3
- [DER] See ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002, Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- [FIPS180] FIPS PUB 180-4, Federal Information Processing Standard, Secure Hash Standard (SHS), March 2012, available at <http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf>
- [FIPS186-3] FIPS PUB 186-3, Federal Information Processing Standard, Dignature Signature Standard (DSS), June 2009, available at [http://csrc.nist.gov/publications/fips/fips186-3/fips\\_186-3.pdf](http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf)
- [FIPS197] Federal Information Processing Standards Publication 197, ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001 available at <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>
- [HboApplCryp] Handbook of Applied Cryptography  
Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone  
CRC Press LLC, Florida, USA, 1997
- [HTTP] RFC 2616, Hypertext Transfer Protocol, HTTP/1.1 (update to RFC 2068), June 1999
- [HTTPS] RFC 2818, E. Rescorla, HTTP over TLS, May 2000, see also [RFC2246]
- [ISO\_IEC\_18032] International Standard ISO/IEC 18032, First edition, 2005-01-15, Information technology – Security techniques – Prime number generation, Geneva, Switzerland 2005
- [KNUT\_CPRG\_II] The Art of Computer Programming, Volume II, Seminumerical Algorithms, 3rd Edition, Donald E. Knuth, Addison Wesley Longman, USA 1998
- [KS2011] Bundesamt für Sicherheit in der Informationstechnik  
Proposal for functionality classes for random number generators, Version 2.0, 2011-09-18
- [PKCS1] PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, June 14, 2002  
see also  
RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications, Version 2.1, RSA Laboratories, February 2003
- [PKCS5] PKCS #5 v2.1, Password-Based Cryptography Standard, RSA Laboratories, October 5, 2006

- [PKCS7] PKCS #7: Cryptographic Message Syntax Standard, Version 1.5, RSA Laboratories, Revised November 1, 1993 available at <ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc>
- [PKCS12] PKCS 12 v1.0: Personal Information Exchange Syntax, RSA Laboratories, June 24, 1999, available at <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf>
- [RFC1321] Request for Comments: 1321, The MD5 Message-Digest Algorithm, April 1992
- [RFC2104] Request for Comments: 2104, HMAC: Keyed-Hashing for Message Authentication, February 1997
- [RFC4346] Request for Comments: 4346, The Transport Layer Security (TLS) Protocol Version 1.1, April 2006
- [RFC4510] Request for Comments: 4510, Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map, June 2006
- [RFC5246] Request for Comments: 5246, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008
- [RFC5280] Request for Comments: 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008
- [SP800-38A] NIST Special Publication 800-38A, 2001 Edition Recommendation for Block Cipher Modes of Operation
- [SP800-90A] NIST Special Publication 800-90A (A Revision of SP 800-90), Recommendation for Random Number Generation Using Deterministic Random Bit Generators, January 2012
- [X9.31] X9.31 - 1998, Digital Signatures Using Reversible Public Key Cryptography ..., American National Standard for Financial Services, American National Standards Institute, September 9, 1998
- [XML] See "W3C Recommendation 04 February 2004, edited in place 15 April 2004", available at <http://www.w3.org/TR/xml11/>

This page was intentionally left blank.

# 11 Appendix/Appendices

Additional documentation texts and references that are related to the above given description.

## 11.1 Appendix A: Overview of HOB RD VPN scenario

