Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0832-2014

for

**HOB RD VPN blue edition
Version 2.1 10.5397**

from

HOB GmbH & Co. KG

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0832-2014

Network and Network related Devices and Systems

HOB RD VPN blue edition
Version 2.1 10.5397

from HOB GmbH & Co. KG

PP Conformance: None

Functionality: Product specific Security Target
Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ALC_FLR.2

Common Criteria Recognition Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 19 February 2014
For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Department

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

SOGIS Recognition Agreement

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product HOB RD VPN blue edition, Version 2.1 10.5397 has undergone the certification procedure at BSI.

The evaluation of the product HOB RD VPN blue edition, Version 2.1 10.5397 was conducted by atsec information security GmbH. The evaluation was completed on 17 February 2014. atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: HOB GmbH & Co. KG.

The product was developed by: HOB GmbH & Co. KG.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

[6] Information Technology Security Evaluation Facility

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product HOB RD VPN blue edition, Version 2.1 10.5397 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] HOB GmbH & Co. KG
Schwadermühlstraße 3
90556 Cadolzburg

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) is the HOB RD VPN blue edition, Version 2.1 10.5397.

The TOE is an encryption secured remote access solution (a so-called SSL-VPN) based on TLSv1.1 and TLSv1.2. The TOE is built of three main components: a gateway called "WebSecureProxy" (WSP), a Java client application for Remote Desktop Services called "HOBLink JWT" and an administrative tool called "HOBLink Security Manager". The TOE provides remote access to Remote Desktop servers and web servers.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
Cryptographic Primitives	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 NIST SP800-90A.
Certificate Generation	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, its use is enforced by the TOE component of the WSP.
Identification, Authentication and Authorization	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 and Remote Desktop servers.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating of the cryptographic algorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

HOB RD VPN blue edition, Version 2.1 10.5397

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	HOB RD VPN blue edition, Version 2.1 10.5397 (whole product containing among others the software parts of the TOE, see Table 3)	Version: 2.1 Revision: 10.5397	DVD
2	DOC	Administration guide HOB Remote Desktop VPN, blue edition, Software Version: 2.1[8] [8]	Version: 1.15	DVD
3	DOC	Administration guide HOBLink Secure and HOBLink Security Manager, Software Version: 3.2 [9]	Version: 1.5	DVD
4	DOC	Security leaflet (READ THIS BEFORE YOU PUT THE CD IN YOUR COMPUTER) [10]	n/a	Hardcopy

Table 2: Deliverables of the TOE

The following table contains the detailed version numbers of the components (Type=C) and modules (Type=M) building the TOE as part of the software product HOB RD VPN blue edition, Version 2.1 10.5397, delivered to the customer on the DVD:

No	Identifier	Release	Type
1	HOB WebSecureProxy	V2.3 Rev.17 Linux EM64T/X86 Oct 28 2013	C
2	HOBLink JWT (including Webstart Module)	3.3.0776	C
3	HOBLink Security Manager	3.2 0090.1174.2710.335	C
4	ServerDataHook: Client Configuration	2.3.0.8	M
5	ServerDataHook: WebServer (including Web Server Gate)	2.3.0.8	M
6	HOBLink Secure SSL Software Module	3.2 0126, Rev. 10.0, 03.12.2013	M

Table 3: TOE components and modules

The product media shipped to the customer contains further components and modules implementing additional product functionality not part of the TOE and therefore not listed here.

[8] The evaluated configuration of the TOE is described in Chapter 30 of this document.

One single DVD containing the software product and the guidance is delivered to the customer. To check the integrity of the content of the delivered DVD, a proprietary software developed by HOB has to be used. The HOB Software Distribution Check[9], running as a signed Java applet is available at the HOB web server under the following URL: https://ftp.hob.de/tools/distribcheck/distribcheckJ2.html.

The URL and instructions required to be performed by the customer in order to verify the integrity of the content of the delivered DVD are documented in the security leaflet also part of the delivery, see table 2). The software compares the hash value generated over the content of the DVD against a stored reference hash value. The reference SHA-256 hash value of the DVD content in hex format is:

70:7C:36:5F:AB:84:00:21:5E:4E:BE:02:DE:57:26:D3:52:3E:EB:6E:31:E3:39:D5:1B:77:18:
56:EF:B8:94:11

The delivery procedure for the TOE is under full control of HOB GmbH & Co. KG in Cadolzburg. Once the customer orders the product, the DVD is put in an appropriate DVD box, labelled with an individual key-code sticker. It contains the product key and the number of licenses and the unique TOE identifier i.e. HOB RD VPN blue edition, Version 2.1, Release 10.5397.

The DVD itself is also labelled with the unique TOE identifier. The DVD box is put in a parcel that in turn is wrapped up in an air-cushioned envelope. The parcel is shipped along with an invoice, a license certificate and a security leaflet to customers by a parcel service. The security leaflet contains instructions required to be performed by the customer in order to verify the integrity of the content of the delivered DVD.

Once the package arrived at the customer's site, the customer is able to verify that the delivery matches the order by reviewing the contents of the invoice as part of the delivery and by cross checking the label on the delivered media. Before installation the customer is instructed to check the integrity of the delivered DVD as described in the security leaflet, using the HOB Software Distribution Checker.

The product version and the software identifiers for all components and specific modules with their version as contained in the compilation of the product are listed in a text file called "RDPVPN_Component_Info.txt" which contains the configuration list of the product. This file is contained on the product DVD that is shipped to the customer. Furthermore, references for the required guidance documentation and non-TOE software parts are contained in this file.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: The TOE is an encryption secured remote access solution and its main purpose is therefore to provide cryptographic primitives, certification generation, the establishment and maintenance of TLS protected links as well as identification, authentication and authorization.

[9] Note that the provided HOB Software Distribution Check has to be used since a special algorithm is implemented to generate the hash value over the whole DVD directory structure.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- The administrators must be competent and trustworthy.
- The LDAP server must implement the functionality required by the TSF correctly and support LDAPv3.
- Information protection procedures must be established and implemented.
- The hardware, software and firmware components must be securely installed.
- The WebSecureProxy must be installed on a separate machine.
- The Security Manager must be installed on a separate machine.
- Critical parts of the TOE must be protected from physical attack.
- The RSA keys must be securely destroyed when they are no longer needed.
- The operating systems, Java virtual machines, and web browsers must be installed and configured in accordance with the guidance.

Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The evaluated configuration of the product is built of three main components "HOB WebSecureProxy", "HOBLink JWT" and "HOBLink Security Manager". The "HOBLink Secure SSL software module” is contained in all three TOE components. It provides all cryptographic functionality required by the TOE. The cryptographic mechanisms implemented by the TOE are shown in table 4. Furthermore the module implements the TLS protocol as specified in [11] for TLSv1.1 and [12] for TLSv1.2. TLS renegotiation is not supported by the TOE. Figure 1 in the Security Target [6] visualizes the architecture of the TOE.

The TOE is composed of:

- The "WebSecureProxy" (WSP) located in front of the destination servers on the gateway server. It is 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. The WSP can handle all incoming connections over one single TCP/IP port.

  The following modules are part of the WSP:

  - HTTP Handler: The module contains the sub-modules "Web Server Gate" and "integrated web server".

    The "integrated web server" passes the user credentials for authentication as entered by the user over an already established HTTPS channel to the LDAP server in the TOE environment, creates the HTTP session cookie assigned to the user after successful authentication and provides the dynamically created start web page to the client containing the URLs to the protected web servers and the links to the protected RD servers the user is authorized to access together with the created cookie.

The "Web Server Gate" establishes the communication with the requested 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 provided by the HTTP handler 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.

- HOBLink Secure, Server: Instance of the HOBLink Secure SSL Software module providing all parts for the TLS protocol at the server side including server authentication (server provides its certificate to the client) and the required underlying cryptographic mechanisms for TLS.

- "HOBLink JWT", a Java Web Start application for Remote Desktop Services that implements the client-side logic ensuring a secured data tunneling for RDP. It shows the GUI of a session to a Remote Desktop server on the local client system.

  The HOBLink JWT application is stored as a HOBLink JWT package in a folder of the RD VPN installation at the gateway server. 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 Web Start application on the client system. I.e. once the user selects a link to a remote desktop server on the start web page presented by the WSP, the JWT Webstart file as provided by the link is downloaded. The HOBLink JWT Webstart file 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 RD VPN. The client HOBLink Security Unit is stored in a folder of the HOB RD VPN installation on the gateway server and is defined in the WSP configuration file. In addition, the HOBLink JWT Webstart file points to the HOBLink JWT package that is to be downloaded by the client's JVM.

  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 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, all subsequent communication with the Remote Desktop server is tunneled through TLS.

  The following module is part of HOBLink JWT:

  - "HOBLink Secure, client": Instance of the HOBLink Secure SSL Software module providing all parts for the TLS protocol at the client side and its required cryptographic mechanisms including server certificate validation. Client authentication via certificates is not foreseen in the evaluated configuration.

- "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.

  It generates the HOBLink Security Units containing the TLS configurations and certificate(s) for the server and those for the client side. The 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 from the HOB WebSecureProxy server component to the HOBLink JWT client via an already established TLS channel.

  The following module is part of HOBLink Security Manager:

  - "HOBLink Secure, client": Instance of the HOBLink Secure SSL Software module providing functionalities for key generation / random number generation and certificate generation (signing of X.509 certificates).

On the client side the browser is not part of the TOE. An initial https connection has to be established to the WSP. During the TLS handshake the WSP authenticates himself with its server certificate and the user has to proof its validity. No client authentication via certificate is foreseen, however when the https connection is established successfully the WSP requires the user first of all to identify and authenticate via user name and password.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

7.1 Developer Testing

Test Configuration

The test environment consists of a WebSecureProxy, which is installed on a SuSE Linux Enterprise Server 11 and the JWT-Clients as well as the Security Manager that are installed on Windows 8, Windows 7, openSuSE Linux 12.2 and Apple Mac OS 10.8.

All test machines except the one running Mac OS X are virtual machines running on VMWare ESX. The test component running Mac OS X is one physical Apple PC.

Tested browsers on the JWT machines are Internet Explorer (IE 10 on Windows 8 and IE 9 on Windows 7), Google Chrome 30.0, and Opera 12.16. As Java Runtime Environment "Oracle Java 1.7.0 update 45" was used.

The installer of the HOBLink Security Manager provides its own Java Runtime Environment. Except the HOB Security Manager, which is installed on Apple Mac OS 10.8 required a manual installation of Apple Java 1.6.0 update 65 (64-bit).

In the test environment in addition an LDAP server supporting the LDAPv3 protocol is set up.

All tools required by the tests, relevant documentation and test results are stored in an SVN repository.

Test Approach
Each test described in the developers' test documentation contains a test case description, its expected result and the test activity with the appropriate test steps and prerequisites.

The test approach consists of a set of manual test cases, which are supported by several tools. The test approach contains some positive tests, such as "connection could be established" and also negative tests, such as "authentication failed with wrong credentials".

The author of the test plan used the security functions provided by the TOE to structure the created test cases, which are covering all aspects of the security functions. In the test plan he organized the tests in chapters representing:

- The "Installation" of the TOE,
- tests covering security functions of the "HOBLink Security Manager",
- the "HOBLink Secure Client (HOBLink JWT)",
- the "HOB WebSecureProxy",
- and a functional test of HOB RDVPN using supported browsers and JREs.
- Last but not least he provided a source code analysis covering the aspects of "Cryptographic key destruction" as an alternative for providing a test case.

Additionally, the developer performs each test case on several operating systems (Windows, Linux, Mac OS) with different parameters on each platform and sometimes in more detail and depth than the Common Criteria i.e. the CEM requires.

Test Results
The tester runs all test steps of each test case and compares this result with the expected result stated in the test case. If the actual test result is equal to the expected result, the tester records a "pass" to his result file. If the results do not match, the tester notes a "fail". The complete test run only gets the verdict "pass" if all test cases get the verdict "pass" during the test execution.

Test Coverage
The functional specification has identified the following TSFI:

- Command Line,
- Client Security Unit,
- WSP Secure Channel,
- Browser HTTPS,
- LDAP,
- Server Security Unit,

- WSP Config and the
- Security Mgr UI.

The tests cover all individual TSFI identified for the TOE.

Test Depth
In addition to the mapping to the functional specification, the developer provided a mapping of TSFI to subsystems of the high-level design. Additionally the evaluator created a mapping of subsystems to appropriate test cases. The evaluator compared those test cases with the test cases of each TSFI that is assigned to the subsystem. The evaluator did not identify any inconsistency, so he considered that the mapping from the subsystems via the TSFI to the test cases demonstrates that all subsystems are implicitly covered by test cases.

Conclusion
The evaluator has verified that developer testing was performed on platforms conformant to the [6].

The evaluator was able to follow and fully understand the developer testing approach by using the information provided by the developer.

The evaluator analysed the developer testing coverage and the depth of the testing by reviewing all test cases. The evaluator found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification as well as the subsystem/internal interfaces identified in the design documentation.

The evaluator reviewed the test results provided by the developer and found them to be consistent with the expected test results according to the test plan.

7.2 Evaluator Testing

Test Configuration
The evaluator used the developer test environment for his independent testing. It was set up by the developer under observation by the evaluator according to the documentation in the Evaluated Configuration Guide which is provided in [8] chapter 30. The tests were performed on virtual machines running on VMWare ESX and one physical Apple PC.

Test Approach, Coverage and Depth
The evaluator testing effort consisted of three parts. The first one is the validation of the test environment that it complies to the evaluated configuration, then the execution of a developer test subset and finally the execution of the tests created by the evaluator.

In addition to running a subset of developer tests, the evaluator devised further tests. The evaluator has chosen these tests for the following reasons:

- The test cases examine some of the security functions of the TOE in more detail than the developer-supplied test cases.
- The test cases cover aspects not included in the developer testing.

In addition to repeating a subset of tests that were provided by the developer according to the test plan from the developer, the evaluator decided to run some additional test cases on the provided test systems:

- Test Tool Verification
- Verify Logging

- Verify LDAP Version
- Cookie Expiration
- Verify HLSECENTROPY can’t be bypassed
- Behavior of the TOE when “/dev/random” is blocking

Test Results

The evaluator verified the configuration against the Evaluated Configuration Guide before conducting the independent tests. The log files of both the executed developer tests and the evaluator tests, generated by the test cases were analysed for completeness and failures. The evaluator determined that the results of the repeated developer tests and additional evaluator tests, performed by the developer and the evaluator together at the developer site, are consistent with the expected results so all tests passed the testing successfully.

7.3 Evaluator Penetration Testing

The evaluator used the TOE set up according to the Evaluated Configuration Guide to conduct the tests. For the code analysis the evaluator used his own workstation and loaded the complete source code and the doxygen archives for WSP and JWT as well as the JAR files for JWT.

The evaluator performed the following analysis and tests:

- Code Analysis
- SSL Vulnerabilities
- Renegotiation
- Handling of the password change field
- Directory Traversal
- Fuzz Testing
- Vulnerability Scan

The analysis of TOE and the TOE configuration has shown that the TOE is not vulnerable in the evaluated configuration in the intended environment.

8 Evaluated Configuration

This certification covers the following configurations of the TOE: The items listed in table 2 of this report represent the TOE. The detailed components and modules of the TOE as part of the product are listed in table 3.

The TOE is composed of three software components:

- HOB WebSecureProxy: The multifunctional VPN gateway (server software)
- HOBLink JWT: A Java web application for Remote Desktop Services (client software)
- HOBLink Security Manager: Administrative management component (software running on a dedicated administration workstation)

All additional software components that are contained in the product are not part of the TOE.

The Security Target [6] states the following requirements for the operational environment of the TOE:

- All TOE components can be run on any kind of machines with Intel Pentium Processors with 1 GHz or other CPU with equivalent speed. The client and administration workstation require volatile memory of at least 256 Mbytes whereas the server component requires 1 Gbyte. Regarding the non-volatile memory the administration workstation requires 160 Mbytes and the server between 250 and 450 Mbytes.
- The server component requires SUSE Linux whereas the client and the administration machine both can be run on Windows 7 and 8, Mac OS X and openSUSE Linux. The hardware and operating system software are not part of the TOE but provide the underlying abstract machine for TOE operation.
- The HOBLink JWT and the HOBLink Security Manager are Java applications requiring a JVM for their execution. For the HOBLink Security Manager running on Windows and Linux the JVM is part of the installation. In case of Mac OS the JVM must be pre-installed (Apple Java 1.6.0 update 65). The client side user is advised to use the most up-to-date Java version provided by Oracle for security reasons. During evaluation it was Oracle Java 1.7.0 update 45. The JVMs are not part of the TOE.
- On the client side a browser supporting TLSv1.1 and TLSv1.2 is required. Currently these are Internet Explorer 9, Opera 12.12 and Google Chrome 29 (version 24 supports only TLS 1.1) or respective higher versions.
- Furthermore an LDAP server is required in the TOE environment to provide Identification services. The LDAP server must support LDAPv3.

The detailed hardware and software requirements are given in [6], section 1.4.1 which is the base for evaluation.

The evaluated configuration of the TOE in its operational environment is defined by the system requirements and mandatory configuration requirements to be met as stated in [8], section 30.5 and 30.6. The Security Target [6] in section 1.5.2.1 redirects readers to this document, which is part of the deliverables listed in table 2.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
EAL 4 augmented by ALC_FLR.2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Confidentiality (TLS bulk data encryption / decryption)	AES in CBC mode	[FIPS197] (AES) [SP800-38A] (CBC)	|k|=128	Yes	TLSv1.1, TLSv1.2
2	Integrity and authenticity (TLS message authentication)	HMAC with SHA-1 or SHA-256	[RFC2104] (HMAC), [FIPS180-4] (SHA)	|k|=160 (SHA-1)	Yes	TLSv1.1, TLSv1.2
				|k|=256 (SHA-256)	Yes	TLSv1.2
3	Key derivation (TLS AES key and MAC key derivation)	HMAC with MD5 combined with SHA-1 or SHA-256	[RFC2104] (HMAC), [RFC1321] and [RFC6151] (MD5), [FIPS180-4] (SHA)	|k|=128 (MD5) combined with |k|=160 (SHA-1)	Yes	TLSv1.1
				|k|=256 (SHA-256)	Yes	TLSv1.2
4	Key establishment (TLS key transport)	RSA encryption and decryption (RSAES-PKCS1-v1-5)	[PKCS#1v2.1] (RSA) [RFC4346] (TLS 1.1), [RFC5246] (TLS 1.2)	modulus length: 1536	No	TLSv1.1, TLSv1.2
				modulus length: 2048	Yes	TLSv1.1, TLSv1.2

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
5	Integrity and authenticity (certificate signing and verification)	RSA signature generation and verification (RSASSA-PKCS1-v 1-5) using SHA-1 or SHA-256	[PKCS#1v2.1] (RSA)	modulus length: 1536	No	certificate generation & certificate validation within TLS
				modulus length: 2048	No (SHA-1)	certificate generation & certificate validation within TLS
					Yes (SHA-256)	certificate generation & certificate validation within TLS
6	Key management	RSA key generation	[FIPS 186-3], B.3.3 and C.3 for Miller Rabin primality tests	modulus length: 1536, 2048	n/a	Please refer to RNG
7	Premaster secret generation	symmetric key generation	-	|k|=384	n/a	Please refer to RNG

Table 4: TOE cryptographic functionality

The TLS1.2 and TLSv1.1 channel has a Security level above 100 Bits (in general context) only if the TOE is configured that for all RSA operations the modulus length is 2048 Bits and SHA-256 is used for the RSA signature generation and verification.

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

In addition, the following aspects need to be fulfilled when installing and using the TOE:

- A parcel with the DVD containing the TOE is shipped along with a security leaflet to the customers by a parcel service. When the customer receives the parcel he is required to follow the instructions contained in the security leaflet in order to check the integrity of the delivered DVD containing the TOE before performing any other action. The instructions contained in the security leaflet are also documented in the Administration Guide HOB Remote Desktop VPN [8], section 30.3, part of the DVD.

- The user is required to ensure that all software not part of the TOE but required by the TOE to function correctly, such as the operating systems of all components as well as the Java virtual machine and the web browser of the remote client, is regularly checked for security updates and kept as up to date as possible. Please refer also to the Administration Guide HOB Remote Desktop VPN" [8], section 30.2, part of the DVD.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JAR	Java Archive
JNI	Java Native Interface
JRE	Java Runtime Environment
JVM	Java Virtual Machine
JWT	Java Windows Terminal
OS	Operating System
PKI	Public Key Infrastructure
PP	Protection Profile
RD	Remote Desktop
RDP	Remote Desktop Protocol

RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionality
VPN	Virtual Private Network
WSP	HOB WebSecureProxy

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

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

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[10].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0832-2014, Version 2.2, 2014-01-15, Security Target for HOB RD VPN blue edition, HOB GmbH & Co. KG

[7] Evaluation Technical Report, Version 5, 2014-02-17, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[8] Administration Guide HOB Remote Desktop VPN, blue edition, Version: 1.15, November 2013

[9] Administration Guide HOBLink Secure and HOBLink Security Manager, Version: 1.5, October 2013

[10] Security leaflet (READ THIS BEFORE YOU PUT THE CD IN YOUR COMPUTER)

[11] RFC4346, Version 1.1, 2006-04-01, The Transport Layer Security (TLS) Protocol, Authors: T. Dierks, E. Rescorla

[12] RFC5246, Version 1.2, 2008-08-01, The Transport Layer Security (TLS) Protocol, Authors: T. Dierks, E. Rescorla

[10] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD:	AGD_OPE.1 Operational user guidance

Assurance Class	Assurance Components
Guidance documents	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.