Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-0260-2004

for

HOBLink Secure, Version 3.1

from

HOB GmbH & Co. KG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0260-2004

HOBLink Secure, Version 3.1

from

HOB GmbH & Co. KG

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL2**

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 27. October 2004

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS-MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-455 - Infoline +49 228 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

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.

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

---

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

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 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, Chech Republic in September 2004.

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 HOBLink Secure 3.1 has undergone the certification procedure at BSI.

The evaluation of the product HOBLink Secure 3.1 was conducted by Tele-Consulting GmbH. The Tele-Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor and developer is 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 on 27. October 2004.

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, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-30.

The product HOBLink Secure 3.1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline 0228/9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] HOB GmbH & Co. KG, Schwadermuehlstraße 3, 90556 Cadolzburg, Germany

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.

Contents of the certification results

1 Executive Summary

The Target of Evaluation (TOE) is HOBLink Secure, Version 3.1.

HOBLink Secure is a software package for integration of SSL/TLS capability into other HOBLink software products such as HOBLink JWT, J-Term or DRDA. It was designed to build a secure communication environment based on three components:

- An administrative tool called “Security Manager” for the generation of configuration files that are required by the two other components.
- A gateway called “WebSecureProxy” located in front of a destination server (referred to as “WSP”).
- A client module called “Java SSL classes”, which works together with an application.

The TOE HOBLink Secure is software only and provides the following security functionality:

- The first service “Certificate Generation” for usage in SSL connections is provided by the software called “SecurityManager”.
- The second service “SSL/TLS Protocol Function” is provided by a set of software components that is able to establish and transfer user data over an SSL connection. This set of components consists of the “SSL Client Classes” and the “WebSecureProxy”.

The evaluated version of the TOE can be run on the following operating systems:

SSL Client Classes (clients):

MS Windows 98SE, NT 4.0 Workstation SP6a, XP Pro, 2000 Pro, 2003

Apple Mac OS 10.3.x

SuSE Linux 8.2, 9.1 (with graphical subsystem installed)

WebSecureProxy (gateway):

HP UX 11i

IBM AIX 5.1

SUN Solaris 9

Security Manager (administration workstation):

MS Windows XP Pro, 2000 Pro, 2003

Apple MacOS, 10.3.x

SuSE Linux 8.2, 9.1 (with graphical subsystem installed)

The hardware requirements for the TOE are the following:

SSL Client Classes (clients):

Intel Pentium 200 MHz or CPU with equivalent processing speed

8 Mbytes of RAM available

WebSecureProxy (gateway):

Intel Pentium III 500 MHz or CPU with equivalent processing speed

64 Mbytes of RAM available

20 Mbytes of non-volatile storage space

Security Manager (administration workstation):

Intel Pentium II 350 MHz or CPU with equivalent processing speed

64 Mbytes of RAM available

40 Mbytes of non-volatile storage space

For a detailed description of the systems the tests were performed on, please refer to chapter 7 of this report.

The product HOBLink Secure 3.1 is delivered by HOB GmbH & Co. KG on CD-ROM or as download on their website.

The scope of delivery of HOBLink Secure 3.1 is shown in the following table:

Component name	**Version**	**Alternate equivalent versions**	
HOBLink Secure (whole product)	3.1	040921	
SSL Client Classes	Version 01.20(9.0)	01.20 040723	
		SSL Version 1 Revision 20 Release 9.0	
		SSL Version 1.20, 23.07.2004	
WebSecureProxy	Version 2.1	On SUN Solaris systems:	2.1 Jun 21 2004
		On HP-UX (IA 64) systems	2.1-pre-02 Aug 4 2004
		On HP-UX (PA RISC) systems:	2.1 Jun 16 2004
		On IBM AIX systems:	2.1 Jun 21 2004

Component name	Version	Alternate equivalent versions
Security Manager	Version 3.1-00.50	3.1 0050
Manual	Version 3.1-0406	-none-

The TOE Security Functional Requirements (SFR) used in the Security Target are Common Criteria Part 2 extended as shown in the following table:

Security Functional Requirement	Identifier
SFRs from CC Part 2	
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ITT.1	Basic internal transfer protection
FDP_ITT.3	Integrity monitoring
FIA_SOS.2	TSF Generation of secrets
Product specific SFRs	
FDP_ITT.EX.1	HOB SSL/TLS Policy

The Security Target specifies one Security Requirement for the IT Environment:

Security Functional Requirement	Identifier
SFRs from CC Part 2	
FPT_STM.1	Reliable time stamps

Note that some of the SFRs have been iterated in the Security Target. For details on the iteration and the required security functionality please refer to the Security Target [6], chapter 5.1.1.

The TOE HOBLink Secure 3.1 was evaluated by:

Tele-Consulting GmbH
Siedlerstraße 22-24
71126 Gäufelden

The evaluation was completed on October 21st, 2004.

The Tele-Consulting GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

[8] Information Technology Security Evaluation Facility

The sponsor and developer is:

HOB GmbH & Co. KG
Schwadermühlstraße 3
90556 Cadolzburg

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C of this report for details).

The TOE meets the assurance requirements of assurance level EAL2 (Evaluation Assurance Level 2).

1.2 Functionality

The TOE HOBLink Secure 3.1 provides the following security functions:

- **Certificate Generation**
  HOBLink Secure 3.1 enforces mutual authentication of the SSL Client Classes component and the WebSecureProxy component of HOBLink Secure 3.1. For this purpose the Security Manager component of HOBLink Secure 3.1 can generate RSA keys and issue X.509v3 certificates according to [9] for these keys with digital signatures based on RSA and SHA-1.

- **SSL/TLS Protocol Function**
  HOBLink Secure 3.1 implements the SSL/TLS protocol. The product does not use third party classes to provide this functionality. The SSL Client Classes component of HOBLink Secure 3.1 reflect the “client” as specified in SSL/TLS and the WebSecureProxy (WSP) component of HOBLink Secure 3.1 implements the “server” as specified in SSL/TLS.

1.3 Strength of Function

In accordance with the requirements of the national scheme no strength of function claim is made for the cryptographic mechanisms and hence for the entire TOE.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

A summary of the threat defined in [6], chapter 3.1.1 is provided here. For the precise description of the threat please refer to [6]:

Name	Description
T.Untrusted-Path	An attacker may attempt 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.

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

The TOE has to comply to the following Organisational Security Policies (OSPs). Note that only a summary of the policies is provided here. For the detailed and precise definition refer to [6], chapter 3.2:

Name	Description
P.Certificates	The TOE must have the ability to generate certificates and the corresponding keys for its own use.
P.Authenticate	The TOE must enforce mutual authentication of the SSL Client Classes component and the WSP component.

1.5 Special configuration requirements

Configuration and installation requirements are detailed in the developer guidance document [8], chapter "The Common Criteria evaluation of HOBLink Secure". The product was designed to ensure that configuration options are as small as possible to get to the evaluated configuration of the TOE.

The following constraints are given by [8]:

- “Client Authentication” for Security Manager is to be used.
- The password file has to be saved to disk.
- The following tools/features which are part of the product were not subject to evaluation and are thus not allowed to be used:
  - Additional tool "SSL for Windows"
  - Java Applet for Installing HLSecurity Units on Clients
  - Additional tool "HOBLink Certificate Generator"
- The use of external certificate stores is not included in the CC evaluation of HOBLink Secure 3.1.
- Several Tabs of the Security manager tool are not part of the evaluation (refer to [8] for more details).
- The configuration evaluated according to CC uses the cipher suite “RSA/AES_128/SHA”.

1.6 Assumptions about the operating environment

The following constraints concerning the allowed hardware and peripherals are made in the Security Target (refer to [6], chapter 2.3):

Hardware Requirements

SSL Client Classes (clients):

Intel Pentium 200 MHz or CPU with equivalent processing speed

8 Mbytes of RAM available

WebSecureProxy (gateway):

Intel Pentium III 500 MHz or CPU with equivalent processing speed

64 Mbytes of RAM available

20 Mbytes of non-volatile storage space

Security Manager (administration workstation):

Intel Pentium II 350 MHz or CPU with equivalent processing speed

64 Mbytes of RAM available

40 Mbytes of non-volatile storage space

Operating Systems

SSL Client Classes (clients):

MS Windows 98SE, NT 4.0 Workstation SP6a, XP Pro, 2000 Pro, 2003

Apple Mac OS 10.3.x

SuSE Linux 8.2, 9.1 (with graphical subsystem installed)

WebSecureProxy (gateway):

HP UX 11i

IBM AIX 5.1

SUN Solaris 9

Security Manager (administration workstation):

MS Windows XP Pro, 2000 Pro, 2003

Apple MacOS, 10.3.x

SuSE Linux 8.2, 9.1 (with graphical subsystem installed)

Java Virtual Machines

Every client has to provide a Java Virtual Machine (JVM). The JVM has to be present stand-alone (for locally installed HOB software) or integrated in a browser (for HOB software in applet-mode).

Most JVMs published since 2000 would be suitable, but the use of the following versions depending on the operating systems is recommended:

Operating system	JVM (local)	Version
MS Windows	SUN MS jview	1.3.1_07 5.00.3167
Apple MacOS X	SUN SUN	1.3.1 1.4.2
Linux	SUN IBM	1.4.1_02 1.3.1

Browsers

Most web browsers that are able to run Java applets would be suitable for use with the SSL Client Classes, but the use of the following software is recommended.

Operating system	Browser	Version
MS Windows	MS Internet Explorer MS Internet Explorer Netscape Netscape Mozilla	5.5 (not on Win XP, 2003) 6 SP1 4.77 (not on Win 2003) 7.1 1.5
Linux	Netscape Mozilla	4.77 1.2.1
Apple MacOS X	MS Internet Explorer Mozilla Safari	5.2.2 1.5 1.2

The following constraints concerning the operating environment are made in the Security Target. The constraints are based on the assumptions defined in [6], chapter 3.3 (Please refer to the Security Target for the precise and more detailed definition):

Name	**Description**
A.Administrators	Administrators are trustworthy, competent and follow all administrator guidance.
A.Users	Authorised users are trustworthy and follow all user guidance.
A.Malicious	All systems shall be free of malicious software such as viruses, trojan horses, worms or spyware.

Name	Description
A.Access	Access to the TOE and to the corresponding systems is limited to authorised persons by appropriate technical, physical and organisational means.
A.SecMgr	The Security Manager has to be installed on a separate machine that is not physically connected to any network and the Security Units generated by this tool are transferred securely between the TOE components.
A.DestroyRSA	RSA keys are securely destroyed when they are no longer needed.
A.Time	The underlying operating system provides reliable time information to the TOE.

1.7 Disclaimers

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 is called:

HOBLink Secure 3.1

The following table summarises the software components of the TOE and defines the evaluated configuration. Please note that no hardware is delivered as part of the TOE:

Component name	**Version**	**Alternate equivalent versions**	
HOBLink Secure (whole product)	3.1	040921	
SSL Client Classes	Version 01.20(9.0)	01.20 040723	
		SSL Version 1 Revision 20 Release 9.0	
		SSL Version 1.20, 23.07.2004	
WebSecureProxy	Version 2.1	On SUN Solaris systems:	2.1 Jun 21 2004
		On HP-UX (IA 64) systems	2.1-pre-02 Aug 4 2004
		On HP-UX (PA RISC) systems:	2.1 Jun 16 2004
		On IBM AIX systems:	2.1 Jun 21 2004
Security Manager	Version 3.1-00.50	3.1 0050	
Manual	Version 3.1-0406	-none-	

The following guidance documents are supplied together with the TOE. The Guidances have to be followed to ensure an certification conformant operation of the TOE: "Product Documentation HOBLink Secure 3.1, Part 1, Version 3.1-0406, September 2004"

3 Security Policy

The TOE is an implementation of the SSL/TLS protocol stack. Its main purpose is therefore to provide a protected communication channel between a client and a server and the generation of the securiy credentials for this channel.

This Security Policy of the TOE is defined by the SFRs as detailed in the Security Target [6], chapter 5.1.1.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the personnel assumptions the following usage conditions exist. Refer to [6], chapter 3.3 for more details:

- Administrators are trustworthy, competent and follow all administrator guidance (A.Administrator).
- Authorised users are trustworthy and follow all user guidance (A.Users).

4.2 Environmental assumptions

The following environmental assumptions defined by the Security Target have to be met (refer to Security Target [6], chapter 3.3):

- All systems shall be free of malicious software such as viruses, trojan horses, worms or spyware (A.Malicious).
- Access to the TOE and to the corresponding systems is limited to authorised persons by appropriate technical, physical and organisational means (A.Access).
- The Security Manager has to be installed on a separate machine that is not physically connected to any network and the Security Units generated by this tool are transferred securely between the TOE components (A.SecMgr).
- RSA keys are securely destroyed when they are no longer needed (A.DestroyRSA).
- The underlying operating system provides reliable time information to the TOE (A.Time).

4.3 Clarification of scope

All threats defined in the Security Target [6], chapter 3.1.1 are countered by the TOE. No threats are defined to be averted by the environment (refer to [6], chapter 3.1.2).

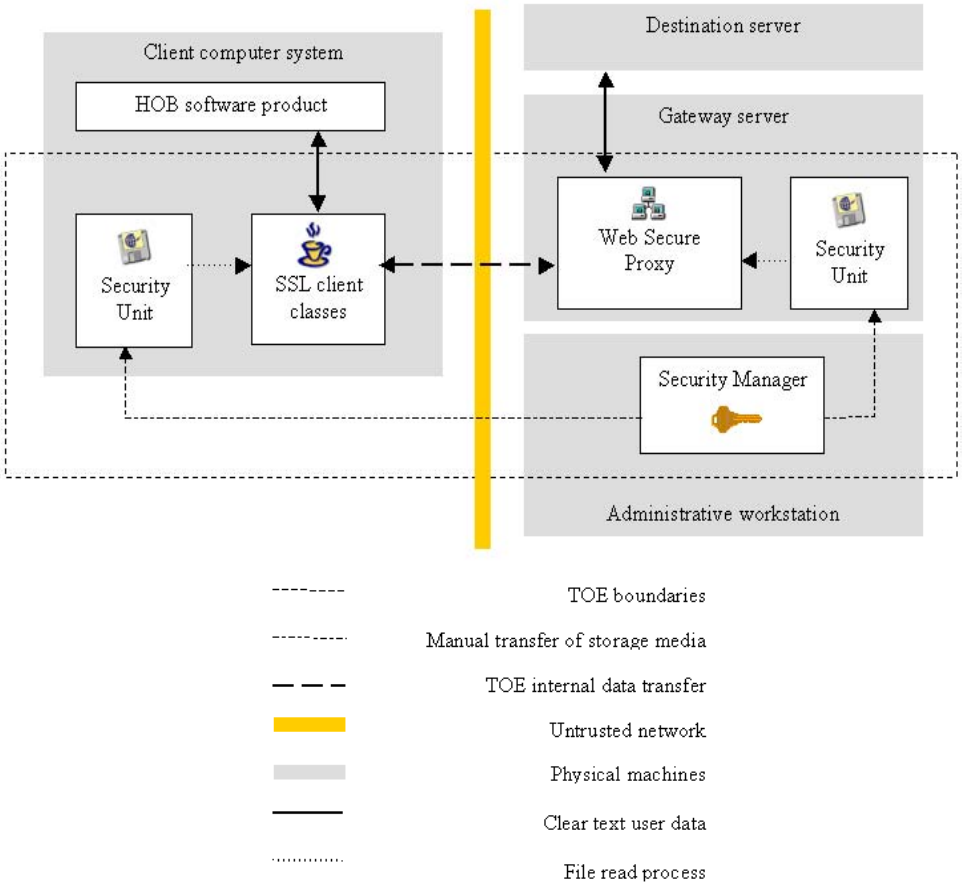
5 Architectural Information

General Overview

HOBLink Secure 3.1 is a software package for integration of SSL/TLS capability into HOBLink software products such as HOBLink JWT, J-Term or DRDA. It was designed to build a secure communication environment based on three components:

- An administrative tool called “Security Manager” for the generation of configuration files (Security Units) that are required by the two other components.
- A gateway called “WebSecureProxy” located in front of the destination server (referred to as “WSP”).
- A client module called “Java SSL classes”, which work together with an application.

The following figure (please refer to [6], chapter 2.2) visualises the systems and components involved, the physical boundary of the TOE, and shows relevant communication paths:



The three components work together as follows:

Before any SSL/TLS connection can be established, the administrator uses the Security Manager to create two sets of configuration files, one for the SSL Client Classes and one for the WSP. Each set of files (referred to as “Security Unit”) consists of three files: The configuration file, the certificate database file and the password file.

The Security Units are manually and securely distributed to the WSP and the client computer which will be using the SSL Client Classes.

The SSL Client Classes are called as soon as an application (for example HOBLink JWT) initiates an SSL/TLS protected connection. The SSL classes read their local Security Unit and initiate an SSL/TLS handshake with the WSP.

The WSP reads its configuration data and the respective Security Units during start up.

When there is an incoming connection request, both parties go through the SSL/TLS handshake procedure and in case of success, the WSP establishes a connection to the destination server system previously defined in the gateway definition file of the WSP.

Security Functions

The security functions of the TOE defined in the Security Target are (refer to Security Target [6], chapter 6.1):

- **Certificate Generation**
  HOBLink Secure 3.1 enforces mutual authentication of the SSL Client Classes component and the WebSecureProxy component of HOBLink Secure 3.1. For this purpose the Security Manager component of HOBLink Secure 3.1 can generate RSA keys and issue X.509v3 certificates according to [9] for these keys with digital signatures based on RSA and SHA-1.

- **SSL/TLS Protocol Function**
  HOBLink Secure 3.1 implements the SSL/TLS protocol. The product does not use third party classes to provide this functionality. The SSL Client Classes component of HOBLink Secure 3.1 reflect the “client” as specified in SSL/TLS and the WebSecureProxy (WSP) component of HOBLink Secure 3.1 implements the “server” as specified in SSL/TLS.

6 Documentation

The following documentation is provided with the product by the developer to the customer:

- Product Documentation HOBLink Secure 3.1, Part 1, Version 3.1-0406, September 2004

7 IT Product Testing

Test configuration

The Security Target [6] defines the following platforms for running the TOE:

SSL Client Classes (clients):

MS Windows 98SE, NT 4.0 Workstation SP6a, XP Pro, 2000 Pro, 2003

Apple Mac OS 10.3.x

SuSE Linux 8.2, 9.1 (with graphical subsystem installed)

WebSecureProxy (gateway):

HP UX 11i

IBM AIX 5.1

SUN Solaris 9

Security Manager (administration workstation):

MS Windows XP Pro, 2000 Pro, 2003

Apple MacOS, 10.3.x

SuSE Linux 8.2, 9.1 (with graphical subsystem installed)

Every client has to provide a Java Virtual Machine (JVM). The JVM has to be present stand-alone (for locally installed HOB software) or integrated in a browser (for HOB software in applet-mode).

The use of the following versions depending on the operating system is recommended by the Security Target:

Operating system	JVM (local)	Version
MS Windows	SUN MS jview	1.3.1_07 5.00.3167
Apple MacOS X	SUN SUN	1.3.1 1.4.2
Linux	SUN IBM	1.4.1_02 1.3.1

The following web browsers are recommended as suitable for use with the SSL Client Classes:

Operating system	Browser	Version
MS Windows	MS Internet Explorer MS Internet Explorer Netscape Netscape Mozilla	5.5 (not on Win XP, 2003) 6 SP1 4.77 (not on Win 2003) 7.1 1.5
Linux	Netscape Mozilla	4.77 1.2.1
Apple MacOS X	MS Internet Explorer Mozilla Safari	5.2.2 1.5 1.2

Depth/Coverage of testing

Although not required by the chosen evaluation assurance level 2 the developer performed testing of the TOE external interfaces. Although not required by the EAL also internal interfaces were tested as necessary. According to the evaluation findings, complete testing coverage was achieved for all the TOE security functions, with the developer tests and the additional tests performed by the independent evaluator testing.

Summary of developer testing efforts

Test configuration:

Tests have been carried out on platforms as described above. Because of the large number of possible combinations of Operating Systems, Browsers and JVMs the developer decided to run the tests on a representative subset. The subset was agreed to be sufficient for developer testing.

Testing approach:

The developer applied an mixed approach of automated and manual tests. Especially the tests covering the interface behaviour of the SSL functionality were collected in an automated test suite.

The test reports were produced by the testing department, which performs independent testing for all HOB products.

Testing was supported by the use of HOB developed tools (test drivers, echo server, error-seeding reverse proxy) and third party tools (network sniffer and analyser).

The test suites addressed “normal processing” as well as behaviour in error situations.

Testing results:

The developer testing for the evaluated configuration of the TOE was performed

successfully on all chosen platforms.

Summary of evaluator testing efforts

Test configuration:

The evaluation facility performed tests on a subset of the platforms listed above. A reasonable argument for the subset chosen was provided. The TOE was setup as required by the the respective guidance documentation.

Testing approach:

The ITSEF has conducted independent testing by repeating developer tests and by performing additional tests, thereby supplementing the TOEs test coverage. In addition also penetration testing was performed by the evaluation facility.

The evaluator has used developer provided tools which were also used for developer testing, a developer provided tool which was provided on request of the evaluator and third party test tools (sniffer, Hex Editor, certificate explorer).

Testing results:

All actual test results obtained by the evaluator matched the expected results.

The penetration tests did not show any obvious vulnerability which was exploitable in the intended environment.

8 Evaluated Configuration

According to the Security Target the evaluated configuration of the TOE is defined as follows (refer also to the Security Target [6] and Product Documentation [8]):

Component name	Version	Alternate equivalent versions	
HOBLink Secure (whole product)	3.1	040921	
SSL Client Classes	Version 01.20(9.0)	01.20 040723	
		SSL Version 1 Revision 20 Release 9.0	
		SSL Version 1.20, 23.07.2004	
WebSecureProxy	Version 2.1	On SUN Solaris systems:	2.1 Jun 21 2004
		On HP-UX (IA 64) systems	2.1-pre-02 Aug 4 2004
		On HP-UX (PA RISC) systems:	2.1 Jun 16 2004
		On IBM AIX systems:	2.1 Jun 21 2004
Security Manager	Version 3.1-00.50	3.1 0050	
Manual	Version 3.1-0406	-none-	

Additional instructions are provided in [8] for an installation according to the CC evaluation of HOBLink Secure 3.1:

- “Client Authentication” for Security Manager is to be used.
- The password file has to be saved to disk.
- The following tools/features which are part of the product were not subject to evaluation and are thus not allowed to be used:
  - Additional tool "SSL for Windows"
  - Java Applet for Installing HLSecurity Units on Clients
  - Additional tool "HOBLink Certificate Generator"
- The use of external certificate stores is not included in the CC evaluation of HOBLink Secure 3.1.
- Several Tabs of the Security manager tool are not part of the evaluation (refer to [8] for more details).
- The configuration evaluated according to CC uses the cipher suite “RSA/AES_128/SHA”.

Configuration and installation requirements are detailed in the developer guidance document [8] "Product Documentation HOBLink Secure 3.1, Part 1, Version 3.1-0406, September 2004" chapter "The Common Criteria evaluation of HOBLink Secure". A user has to follow the instructions given in the chapter

"The Common Criteria evaluation of HOBLink Secure" to get the evaluated configuration of the TOE.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Common Evaluation Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The verdicts for the CC, Part 3 assurance components (according to EAL2 and the Security Target evaluation) are summarised in the following table:

Assurance Classes and Components		Verdict
Security Target	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Configuration items	ACM_CAP.2	PASS
Delivery and Operation	CC Class ADO	PASS
Delivery Procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Descriptive high-level design	ADV_HLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Tests	CC Class ATE	PASS
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

The TOE has no obvious vulnerabilities which are exploitable in the intended operating environment.

The results of the evaluation are only applicable to the product HOBlink Secure 3.1 in the configuration as defined in the Security Target and summarised in this report (refer to the Security Target [6] and the chapters 2, 4, 6 and 8 of this report).

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, and if the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The Guidance documentation (refer to chapter 6) contains necessary information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [6] and the Security Target as a whole has to be taken into account. Therefore a user/administrator has to follow the guidance in these documents.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete security target [6] used for the evaluation performed.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

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

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

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-0260-2004, Version 1.7, 14.09.2004, Security Target for HOBLink Secure 3.1, HOB GmbH & Co. KG

[7] Evaluation Technical Report for HOBLink Secure 3.1, Version 2, 21.10.2004, Tele-Consulting GmbH (confidential document)

[8] Product Documentation HOBLink Secure 3.1, Part 1, Version 3.1-0406, September 2004

[9] Housley, R., Ford, W., Polk, W. and D. Solo, Internet Public Key Infrastructure: Part I: X.509 Certificate and CRL Profile, RFC 2459, January 1999

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„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 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 6.1)

Table 6.1 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 2 of this 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 CC 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„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 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, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„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 practice. 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 6.2.3)

„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 practices.

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 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 6.2.6)

„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 6.2.7)

„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.“

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.“

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.“

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.“

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“