CERTIFICATION REPORT

Certification file:	**TUVIT-DSZ-CC-9252**
Product / system:	VPN software directVPN Zugangssoftware, Version 5.3
Product manufacturer:	T-Online International AG T-Online-Allee 1 64295 Darmstadt
Customer:	see above
Evaluation facility:	secunet SwissIT AG, evaluation body for IT security Hauptbahnhofstr. 12, CH-4501 Solothurn, Switzerland
Evaluation report:	*Version 1.2 as of 2006-02-21* Document-number: *9252ETR-1.2.odt* Author: Dr. Susanne Röhrig
Result:	EAL1
Evaluation stipulations:	one (see chapter 10)
Certifier:	Dr. Christoph Sutter
Certification stipulations:	one (see chapter 11)

Essen, 2006-02-24

Dr. Ernst-Hermann Gruschwitz Dr. Christoph Sutter

Contents

Part A

Certificate and Background of the Certification

Part A presents a copy of the issued certificate and summarizes

- information about the certification body,
- the certification procedure, and
- the performance of evaluation and certification.

1 The Certificate

Deutsches
IT-Sicherheitszertifikat
anerkannt vom
Bundesamt für Sicherheit in der Informationstechnik

CER TÜViT

The Certification Body of TÜV Informationstechnik GmbH
hereby certifies that the VPN software

directVPN Zugangssoftware, Version 5.3
of
T-Online International AG

has been evaluated at an accredited and licensed/approved evaluation facility using the *Common Methodology for IT Security Evaluation (CEM) Part 1 Version 0.6* and *CEM Part 2 Version 2.2* for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.2* with the following results:

SECURITY FUNCTIONALITY
Product specific Security Target
Common Criteria part 2 conformant

ASSURANCE PACKAGE
Common Criteria part 3 conformant
EAL 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 recommendations and stipulations in the certification report must be respected. The evaluation has been conducted in accordance with the provisions of the certification scheme of TÜV Informationstechnik GmbH and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The security target, against which the product has been evaluated, is part of the certification report. The rating of the strength of cryptographic mechanisms suitable for encryption and decryption is excluded from the recognition by BSI. A copy of the certificate and of the certification report is available from the product manufacturer or from the certification body.

This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH or by any other organisation that recognises or gives effect to this certificate is either expressed or implied.

Certificate-Registration-No.
TUVIT-DSZ-CC-9252-2006

Essen, 2006-02-24 sign. Dr. Gruschwitz
Certification Body

TÜV Informationstechnik GmbH – Member of TÜV NORD Group • Langemarckstraße 20 • 45141 Essen, Germany
☎ +49 201 8999-580 • 🖷 +49 201 8999-555 • certuvit@tuvit.de • www.certuvit.de
accredited for IT security certifications under DAR-registration no. DAT-ZE-014/99-01 by
Deutsche Akkreditierungsstelle Technik GmbH (DATech)

2 Certification Body – CERTÜViT

CERTÜViT, the Certification Body of *TÜV Informationstechnik GmbH*[1] – Member of TÜV NORD Group – was established in 1998 and offers a variety of services in the context of security evaluation and validation.

CERTÜViT was accredited in September 1999 for certification of IT security products according to ITSEC and Common Criteria by *Deutsche Akkreditierungsstelle für Informations- und Telekommunikationstechnik (Dekitz)* now *Deutsche Akkreditierungsstelle Technik GmbH (DATech), Frankfurt/Main* under DAR-registration no. DAT-ZE-014/99-01 and performs its projects under a quality management system certified against ISO 9001 by *Germanischer Lloyd, Hamburg*.

CERTÜViT is accredited by *Bundesamt für Sicherheit in der Informationstechnik*[2] to issue the "German IT Security Certificate" which is recognised by BSI as equivalent to the "German IT Security Certificate" of BSI.

3 Specifications of the Certification Procedure

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

- DIN EN 45011
- TÜViT Certification Scheme
- TÜViT Certification Conditions
- Regulations on the "German IT Security Certificate" issued by the BSI and accepted in the contract of BSI and TÜViT as of November 20, 2002.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, version 2.2, January 2004.
- Common Methodology for Information Technology Security Evaluation (CEM) part 1, version 0.6, January 1997.
- Common Methodology for Information Technology Security Evaluation (CEM) part 2, version 2.2, January 2004.
- Application Notes and Interpretations of the Scheme (AIS), published by BSI.

[1] in the following termed shortly TÜViT

[2] in the following termed shortly BSI

4 Recognition Agreements

In order to avoid multiple certification of the same product by different certification bodies a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed. CERTÜViT certificates are German IT Security Certificates recognized by BSI – the national German certification body in international agreements – to be equivalent to its own certificates but they are not part of these international agreements.

4.1 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4 was signed between the national participants of Australia and New Zealand, Austria, Canada, Czech Republic, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, The Netherlands, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom and the United States.

4.2 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. The arrangement on the mutual recognition of IT security certificates based on the CC was extended by these participants up to and including the evaluation assurance level EAL7.

5 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The VPN software *directVPN Zugangssoftware, Version 5.3* has undergone the certification procedure at TÜViT certification body. It was a re-certification of the directVPN Zugangssoftware, Version 4.5.50 (TUVIT-DSZ-CC-9239-2005 as of 2005-10-06) due to changes in the drop-down menus, supported operating systems, and needed ports for the communication.

The evaluation of the VPN software directVPN Zugangssoftware, Version 5.3 was conducted by the evaluation body for IT-security of secunet SwissIT AG and concluded on February 21, 2006. The secunet SwissIT AG evaluation facility is recognised by BSI.

The sponsor as well as the developer is T-Online International AG. Distributor of the product is T-Online International AG.

The certification was concluded with

- the comparability check and
- the preparation of this certification report.

This work was concluded on February 24, 2006. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stipulations regarding generation, configuration and operation, as given in part B of this report, are observed,
- the product is operated – where indicated – in the environment described.

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

With regard to the meaning of the evaluation assurance levels (EAL) and the strength of function (SoF), please refer to part C of this report.

6 Publication

The following Certification Results consist of pages B-1 to B-15. The product directVPN Zugangssoftware, Version 5.3 will be included in the BSI list of certified products which is published at regular intervals (e. g. in the Internet at http://www.bsi.bund.de) and the TÜViT certification lists (http://www.certuvit.de).

Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form at the internet address of CERTÜViT as stated above.

Part B

Certification Result

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 Result

1 Executive Summary

1.1 Target of Evaluation and Evaluation Background

The target of evaluation (TOE) is the VPN software ***directVPN Zugangssoftware, Version 5.3***. The TOE is a part of the directVPN Software Suite, a software component used to establish an encrypted connection (secure channel) between a common PC and another PC joining the same Virtual Community Network (VCN). The VCN is a special type of enhanced Virtual Private Network (VPN) also called in this context directVPN.

The directVPN solution creates a network services layer above the flat Internet address space allowing the creation of dynamic communities. This layer facilitates the introduction of network services with centralized management such as VPN or IP-telephony domains.

An overview about the components of the directVPN solution is given in the following figure:

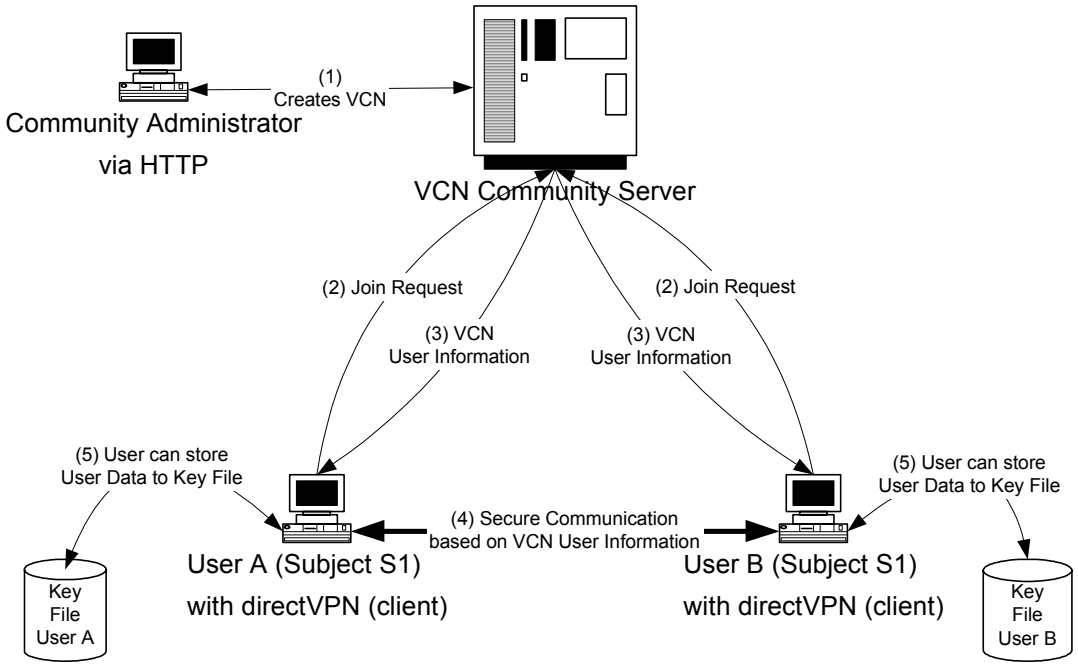

Figure 1: Overview about the directVPN solution. The TOE is part of the directVPN (client).

In establishing a Virtual Community Network (VCN), the provider (T-Online International AG), sets up a VCN Community Server and assigns one or more of their representatives to administer the VCN Community Server.

In establishing a VCN the community administrator registers at the T-Online International AG the new community and creates the VCN within their customer domain (figure 1, (1)). The community administrator pre-registers all members in the VCN and transmits all necessary information – including the VCN password – to them.

Once registered in a VCN, the member is classified as either an active or inactive member of the VCN. An inactive member can send a Join Request to the VCN Community Server. The server ensures that only registered members of a VCN can join the VCN (figure 1, (2)) and can become an active member of the VCN. This is done in the following way: During registration membership information for that VCN are downloaded and stored in a User Information File, which is maintained on the hard drive of the PC. The membership information includes the information necessary to identify to the VCN Community Server as a registered member of the VCN. Active members get information about all other active members (figure 1, (3)) and can establish a secure connection with another active member of the same VCN (figure 1, (4)).

After submitting a Leave Request to the VCN Community Server, an active member leaves the VCN and becomes an inactive member.

Within the focus of the evaluation and certification are the following two security features:

- The TOE can establish a secure channel (figure 1, (4)) between two active VCN members of the same VCN that protects the exchanged application data in confidentiality and integrity.
- The TOE can export membership information encrypted into a key file (figure 1, (5)). The used encryption key is derived from a password entered by the user. The membership information can be imported after presenting the correct password.

The directVPN (client) has further functionality that is **not** within the scope of evaluation:

- Graphical User Interface (GUI) for communicating with the VCN Community Server including the service requests: Join, Query, Leave, Change Password, Import/Export membership information, and Secure File Sharing Request.
- Secure communication with the VCN Community Server.
- Host-to-host exchange of encrypted IP packets with the VCN Community Server.
- Member authentication using Digital Certificates.
- Establish connections by other applications (such as telnet, ftp, or browser) with other active members.
- Download of changes to the member's User Information File when the member joins the VCN.
- Secure File Sharing between VCN Members.
- Online user help information (e.g. Help Pages, contact information, etc.).

1.2 Assurance Package

The TOE security assurance requirements are based entirely on the assurance components and classes defined in Part 3 of the Common Criteria (see part C of this report or [CC] Part 3 for details). The TOE meets the assurance requirements of assurance level EAL 1 (Evaluation Assurance Level 1).

1.3 Strength of Functions

The assurance component AVA_SOF.1 “Strength of TOE security functions (AVA_SOF)” is not part of the present evaluation level EAL 1.

1.4 Functionality

All TOE security functional requirements were taken from CC part 2 (i. e. the set is CC part 2 conformant) [CC]. They can be categorized into the following four functional classes:

1. cryptographic support,
2. user data protection,
3. identification and authentication, and
4. trusted path/ channel.

Chapter 9 lists the security functional requirements in more detail. They are met by two suitable TOE security functions (TSF):

TSF	Short Description
Key File-Access	provides an encrypted and integrity protected export / import of membership information to / from a key file
Secure Channel	provides a secure channel for exchange of application data with another directVPN client of the same VCN

A more detailed description of the TOE security functions can be found in section 6.1 of the public ST, which is attached as part D of this certification report.

1.5 Summary of Threats and Organisational Security Policies (OSPs)

The main assets for the TOE are integrity and confidentiality of membership information when stored in the key file (figure 1 (5)) as well as integrity and confidentiality of application data when transferred in the secure channel (figure 1 (4)) between two directVPN (client).

The attacker may be any person apart from the TOE user that tries to compromise the assets. Two threats deal with the loss of integrity or confidentiality of application data transmitted between two directVPN (client). The other two threats deal with the loss of integrity or confidentiality of membership information stored in the key file.

The Security Target [ST] does not specify any organisational security policy.

A more detailed description of the threats can be found in section 3.3 of the public ST, which is attached as part D of this certification report.

1.6 Special Configuration Requirements

The TOE is delivered in one fixed configuration that is part of the certification.

1.7 Assumptions about the Operating Environment

The TOE must be used in the environment described in section 1.1 and figure 1. The operating environment for the PC of the directVPN (client) where the TOE is installed must include the following:

- Platform(s): PC with 128 MB of RAM (minimum)
- Processor: Intel/AMD 32-bit x86 based PC, 233 MHz or higher
- Operating system: Windows XP Home Edition, Windows XP Professional, Windows 2003 Server, Windows 2000, Windows 2000 Server
- Physical Location: Any network with public Internet access
- Network Access: Private network or direct Internet connection
- Firewall (to prevent attacks from the internet)
    - Ports (default, must be allowed by the firewall): TCP: 80, 433; UDP: 20202
- Web Browser compatible to Internet Explorer 5.5 or Firefox 1.5 to display Help-pages
- Requires Fixed IP(s): No

Further assumptions about the environment of use are contained in chapter 4.

1.8 Independence of the Certifier

Within the last two years, the certifier did not render any consulting- or other services for the company ordering the certification and there was no relationship between them that might have an influence on his assessment.

The certifier did not participate at any time in test procedures for the product, which forms the basis of the certification.

1.9 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 with regard to generation, configuration and operation as detailed in this certification report. This certificate is not an endorsement of the IT product by TÜV Informationstechnik GmbH or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Informationstechnik GmbH 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) *directVPN Zugangssoftware, Version 5.3* and the user documentation is included in the setup file “dvpnclient.exe”. The file is delivered on a CD-ROM or can be downloaded from the web-site of T-Online International AG (ftp://software.t-online.de/pub/service/directvpn/dvpnclient.exe). The SHA-1 hash value of the file is:

- `3e 65 a0 9e 80 7b ff 92 1a bb 17 83 3b 9f b7 7d 3f 87 2e 01`

3 Security Policy

Within the security target one single security policy is defined:

Policy Name	Description
AC SFP	import and export of membership information from/to a key file is done in a confidential and integer way and protected by a password

A more detailed description of the security policy can be found in section 5.1 of the public ST, which is attached as part D of this certification report.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The only assumptions defined in the ST are assumptions about the environment of use (see following section). There is no usage assumption defined in the ST.

4.2 Environmental Assumptions

The following six assumptions about the environment of use are defined in the ST and must be regarded when using the TOE.

Assumption	Description
A.ADMIN	It must be assumed that competent and trustworthy community administrators are assigned as required.
A.MEMBERSHIP_ INFORMATION	It must be assumed that the membership information was created by community administrators and transmitted to the directVPN Zugangssoftware before initiating a connection. It must be assumed that the membership information is used in a correct way to register and to join at the VCN.
A.SECURE_MI_ EXPORT	The VCN Community Server supports a secure channel capability (providing confidentiality, data integrity, and VCN Community Server Authentication) to export the membership information from VCN Community Server to the directVPN Zugangssoftware in a secure way. This information is stored on the directVPN Zugangssoftware PC.
A.AVAILABLE	It must be assumed that Internet or other required public network connections are available to the TSF when required.
A.PROTECTION	It must be assumed that the directVPN Zugangssoftware PC is protected sufficiently (using virus scanning tools and firewalls) against malicious code or direct attacks which may be used to harm the security functions of the TOE.
A.AUTHORISATION	Before establishing a connection to another directVPN Zugangssoftware the VCN Member has to be authenticated by the VCN Community Server in that way that the VCN Member has to provide the right VCN Password. The VCN Community Server ensures that only authorized VCN Member Agents can establish a secure channel within in a VCN (to the VCN Community Server, to another directVPN Zugangssoftware) and are contained in the list of active VCN member agents.

4.3 Clarification of Scope

Within the focus of the evaluation and certification are only the following two security features:

- The TOE can establish a secure channel (figure 1, (4)) between two actives VCN members of the same VCN that protects the exchanged application data in confidentiality and integrity.
- The TOE can export membership information encrypted into a key file (figure 1, (5)). The used encryption key is derived from a password entered by the user. The membership information can be imported after presenting the correct password.

The directVPN (client) software has further functionality that is **not** within scope of the evaluation:

- Graphical User Interface (GUI) for communicating with the VCN Community Server including the service requests: Join, Query, Leave, Change Password, Import/Export membership information, and Secure File Sharing Request.
- Secure communication with the VCN Community Server.
- Host-to-host exchange of encrypted IP packets with the VCN Community Server.
- Member authentication using Digital Certificates.
- Establish connections by other applications (such as telnet, ftp, or browser) with other active members.
- Download of changes to the member's User Information File when the member joins the VCN.
- Secure File Sharing between VCN Members.
- Online user help information (e.g. Help Pages, contact information, etc.).

5 Architectural Information

For the present evaluation level EAL 1 no information concerning the architecture of the TOE is available.

6 Documentation

The (online) user documentation

- Hilfe zur directVPN Zugangssoftware (Version 4.4 oder höher)

is included in the program code of directVPN Zugangssoftware, Version 5.3.

7 IT Product Testing

Developer tests were not performed as they are not required for evaluation assurance level EAL 1.

The evaluation body performed independent testing on the five relevant statements of both TSF. These statements were considered to describe the core functionality of the TOE and to be the most important aspects. All test results were consistent with the expected results showing that the TOE behaved as specified in the TSF.

8 Evaluated Configuration

The TOE is delivered in one fixed configuration and no further generation takes place. Therefore the evaluated configuration is identical to the TOE, which can be identified as described in chapter 2 of this certification report.

9 Results of the Evaluation

The Evaluation Technical Report [ETR] was provided by secunet SwissIT AG's evaluation body according to the requirements of the Scheme, the Common Criteria [CC], the Methodology [CEM] and the Application Notes and Interpretations of the Scheme [AIS].

The verdicts for the CC, part 3 assurance classes and components (according to EAL1 and the class ASE for the Security Target Evaluation) are summarised in the following table:

Assurance classes and components		**Verdict**
Security Target evaluation	**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
Version numbers	ACM_CAP.1	PASS
Delivery and operation	**CC Class ADO**	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	**CC Class ADV**	PASS
Informal functional specification	ADV_FSP.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
Independent testing – conformance	ATE_IND.1	PASS

All assurance components were assessed with the verdict PASS. This includes that all evaluator action elements being part of the assurance components are also assessed with PASS. Therefore, the TOE as defined in the security target is considered to be Part 3 conformant.

Section 5.1 of the public ST, which is attached as part D of this certification report, lists the following TOE security functional requirements.

ID	**Class**/Component
FCS	**Cryptographic support**
FCS_CKM.1	Cryptographic key generation
FCS_COP.1	Cryptographic operation
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of user data without security attributes
FIA	**Identification and authentication**
FIA_SOS.1	Verification of secrets
FTP	**Trusted Path/channels**
FTP_ITC.1	Inter-TSF trusted channel

All security functional requirements were taken from [CC] part 2, i. e. the TOE is [CC] part 2 conformant.

The evaluation performed in accordance to EAL1 has shown that the TOE security functional requirements are correctly realised by the TOE security functions. Thus, in realising these functional requirements, it is assured that the TOE will meet the security objectives claimed in the ST.

The assurance component AVA_SOF.1 “Strength of TOE security functions (AVA_SOF)” is not part of the present evaluation level EAL 1 and no minimum strength of function level is specified.

The sponsor must advise the certification authority about any modification of the TOE or its guidance documentation. The certification authority will then check whether the certification results are still valid and, if necessary, initiate all further steps concerning a re-evaluation.

The results of the evaluation are only applicable to the product "*directVPN Zugangssoftware, Version 5.3*". 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.

10 Evaluation Stipulations, Comments, and Recommendations

The evaluation report contains the following stipulation for the user:

- The user of the directVPN Zugangssoftware, Version 5.3 has to assure that their PC is protected sufficiently using anti-malware software (i. e. virus scanning tools and firewalls) against malicious code or direct attacks which might harm the security functions of the TOE.

The evaluation report does not contain any evaluation comments or recommendations.

11 Certification Stipulations and Notes

The stipulation of the evaluation report (see chapter 10) is applicable. There are no additional notes or stipulations resulting from the certification report.

There are no certification stipulations or notes.

12 Security Target

The public version [ST-lite] of the security target [ST] for *directVPN Zugangssoftware, Version 5.3* is included in part D of this certification report.

13 Definitions

13.1 Acronyms

ADM	Administrator Guidance
API	Application Programming Interface
CC	Common Criteria for Information Technology Security Evaluation (referenced to as [CC])
CEM	Common Methodology for Information Technology Security Evaluation (referenced to as [CEM])
CM	Configuration Management
EAL	Evaluation Assurance Level
FSP	Functional Specification
HLD	High-level Design
IF	Interface
IGS	Installation, Generation and Start-up
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIF	Sub-interface
SOF	Strength of Function
SS	Sub-system
ST	Security Target
TOE	Target Of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Function Interfaces
TSP	TOE Security Policy
USR	User Guidance
VCN	Virtual Community Network
VLA	Vulnerability Analysis
VPN	Virtual Private Network

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from 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

[AIS] Application Notes and Interpretations of the Scheme (AIS), published by BSI

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004,
Part 1: Introduction and general model
Part 2: Security functional requirements
Part 3: Security assurance requirements

[CEM] Common Methodology for Information Technology Security Evaluation,
Part 1: Introduction and general model, version 0.6, revision 11.01.1997,
Part 2: Evaluation Methodology, version 2.2, January 2004

[ETR] Evaluation Technical Report, secunet SwissIT AG,
version 1.2, 2006-02-21, document-number: 9252ETR-1.2.odt

[ST] Security Target for directVPN Zugangssoftware, Version 5.3, Version 01.01, 2006-02-15
confidential document

[ST-lite] Security Target Lite for directVPN Zugangssoftware, Version 5.3, Version 01.01, 2006-02-15
public version of the Security Target [ST]

Part C

Excerpts from the Criteria

The excerpts from the criteria are dealing with

- conformance results
- assurance categorization
- evaluation assurance levels
- strength of security function
- vulnerability analysis

CC Part 1:

Conformance results

„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 predefined 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

The assurance classes, families, and the abbreviation for each family are shown in *Table 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 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

„Table 2 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 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 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_IMT					**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 2: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested

“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

“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

“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

“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

“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

“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

“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)

AVA_SOF Strength of TOE security functions

“Strength of function analysis addresses TOE security functions that are realised by a probabilistic or permutational mechanism (e.g. a password or hash function). Even if such functions cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat them by direct attack. A level or a specific metric may be claimed for the strength of each of these functions. Strength of function analysis is performed to determine whether such functions meet or exceed the claim. For example, strength of function analysis of a password mechanism can demonstrate that the password function meets the strength claim by showing that the password space is sufficiently large.”

Three levels exist: SOF-basic, SOF-medium, and SOF-high.

Vulnerability analysis (AVA_VLA)

AVA_VLA Vulnerability analysis

"Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: (1) the completeness of the TSF (does the TSF counter all the postulated threats?) and (2) the dependencies between all security functions. These potential vulnerabilities are assessed through penetration testing to determine whether they could, in practice, be exploitable to compromise the security of the TOE."

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.

The intent of the developer analysis is to confirm that no identified security vulnerabilities can be exploited in the intended environment for the TOE and that the TOE is resistant to obvious penetration attacks.

Obvious vulnerabilities are considered to be those that are open to exploitation that requires a minimum of understanding of the TOE, skill, technical sophistication, and resources. These might be suggested by the TSF interface description. Obvious vulnerabilities include those in the public domain, details of which should be known to a developer or available from an evaluation authority.

Performing a search for vulnerabilities in a systematic way requires that the developer identify those vulnerabilities in a structured and repeatable way, as opposed to identifying them in an ad-hoc fashion. The associated evidence that the search for vulnerabilities was systematic should include identification of all TOE documentation upon which the search for flaws was based.

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. To accomplish this intent, the evaluator first assesses the exploitability of all identified vulnerabilities. This is accomplished by conducting penetration testing. The evaluator should assume the role of an attacker with a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential when attempting to penetrate the

TOE. Any exploitation of vulnerabilities by such an attacker should be considered by the evaluator to be “obvious penetration attacks” (with respect to the AVA_VLA.*.2C elements) in the context of the components AVA_VLA.2 through AVA_VLA.4.”

Part D

Security Target

Attached is the public version of the Security Target: "*Security Target Lite for directVPN Zugangssoftware*"

Author: T-Online International AG

Date: 2006-02-15

Version: 01.01