CERTIFICATION REPORT

Certification file:	**TUVIT-DSZ-CC-9239**
Product / system:	VPN software directVPN Zugangssoftware, Version 4.5.50
Product manufacturer:	T-Online International AG T-Online-Allee 1 64295 Darmstadt
Customer:	see above
Evaluation facility:	TÜViT, evaluation body for IT security
Evaluation report:	*Version 2.0 as of 2005-06-06* Document-number: *20648411_TÜViT_008.2* Author: Christoph Zurheiden
Result:	EAL1
Evaluation stipulations:	one (see chapter 10)
Certifier:	Dr. Christoph Sutter
Certification stipulations:	one (see chapter 11)

Essen, 2005-06-10

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

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

directVPN Zugangssoftware, Version 4.5.50
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-9239-2005

Essen, 2005-06-10 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 • 🖂 tuvit@tuvit.de • 🌐 www.certuvit.de
accredited for IT security certifications under DAR-registration no. DIT-ZE-014/99-00 by
Deutsche Akkreditierungsstelle Technik e.V. (DATech)

2 Certification Body – CERTÜVIT

CERTÜVIT, the Certification Body of *TÜV Informationstechnik GmbH*[1] – a 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 e.V. (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, 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 4.5.50* has undergone the certification procedure at TÜViT certification body. It was an initial certification.

The evaluation of the VPN software directVPN Zugangssoftware, Version 4.5.50 was conducted by the evaluation body for IT-security of TÜViT and concluded on June 6, 2005. The TÜViT 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 June 10, 2005. 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 4.5.50 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 4.5.50***. 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:

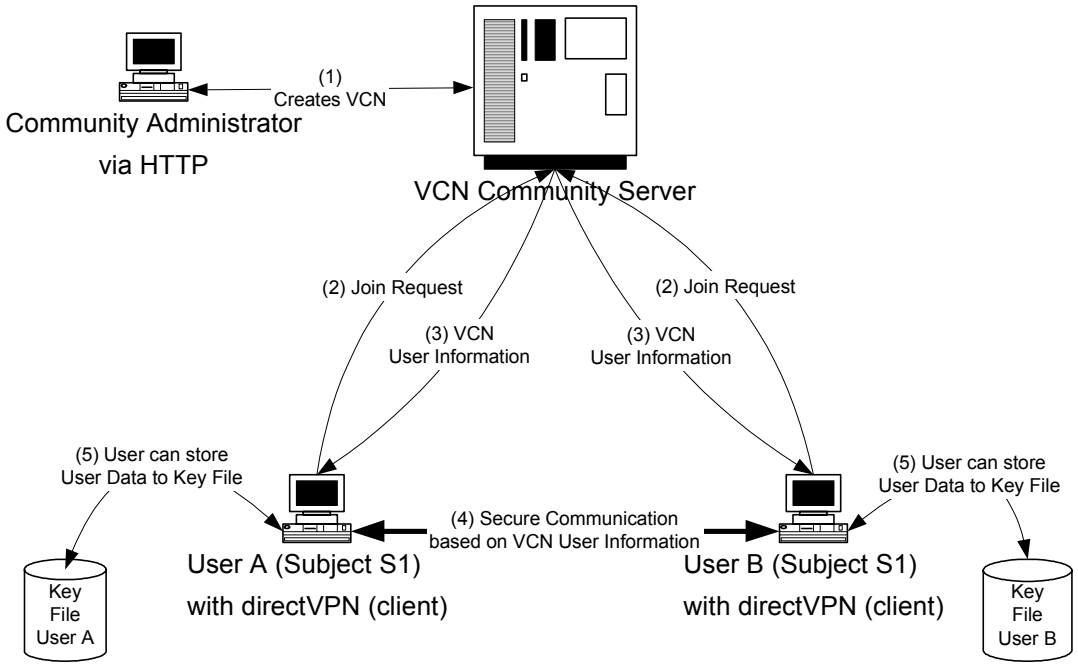

Figure 1: Overview about the directVPN solution. The TOE is part of the directVPN (client).

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 64 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 2000, Windows 98 SE, Window 2000 Advanced Server
- Physical Location: Any network with public Internet access
- Network Access: Private network or direct Internet connection
- Firewall (to provide attacks from the internet)
    - Ports (default, must be allowed by the firewall): TCP: 80, 433, 900, 9001, 9002; UDP: 20202
- Web Browser compatible to Internet Explorer 5.5 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 4.5.50* 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:

- `5a 3d dd 5f 9a 70 6c 4d 70 a9 8f 05 7f 6e 06 b3 02 2a 6c a6`

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 4.5.50.

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 TÜViT'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 4.5.50*". 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 has to assure that the 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.

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 4.5.50* 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, TÜV Informationstechnik GmbH,
version 2.0, 2005-06-06, document-number: 20648411_TÜViT_008.2

[ST] Security Target for directVPN Zugangssoftware, Version 4.5.50, Version 00.02.07, 2005-05-10
confidential document

[ST-lite] Security Target Lite for directVPN Zugangssoftware, Version 4.5.50, Version 1.0, 2005-05-18
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 (section 5.4 of CC part 1 with 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 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.“

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 for directVPN Zugangssoftware, Version 4.5.50*

Author: T-Online International AG

Date: 2005-05-18

Version: 1.0

Security Target Lite
for
directVPN Zugangssoftware, Version 4.5.50,

a Product of
T-Online International AG

Version:	1.0
Date:	2005-05-18
Doc. ID:	ST Lite-directVPN Zugangssoftware
File Name:	directVPN_ST Lite.doc
Author(s):	secunet Security Networks AG
Certif. ID:	TUVIT-DSZ-CC-9239

Document Identification

ST-Name:	ST Lite -directVPN Zugangssoftware
ST-Version:	1.0
Date:	2005-05-18
Author:	secunet Security Networks AG
TOE-Name/-Version:	directVPN Zugangssoftware, Version 4.5.50.
CC-Version:	2.1
EAL	EAL1 according to [CC]

Table of Contents

List of Tables

1 ST Overview

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 Virtual Private Networks (VPN) or IP-telephony domains.

The Virtual Community Network (VCN) is a special type of enhanced VPN. In this document this term is often used in context with directVPN.

The Virtual Domain Network™ (VDN™) technology on which the VCNs are based allows Internet users to route encrypted IP packets from source to destination (i.e., end-to-end) when the source and destination devices are in different addressing realms.

Leveraging industry-standard DNS-type naming, directVPN provides true peer-to-peer (endpoint-to-endpoint) encryption to deliver more manageable, highly scalable, very secure business communications.

- The directVPN Zugangssoftware is as a part of the directVPN Software Suite a software component used to get an encrypted connection (secure channel) between a common PC and another PC joining the same VCN. Several features serve measures to authenticate the directVPN Zugangssoftware against a VCN Community Server so that only VCN-members can communicate with each other. Those security measures are provided by these VCN Community Servers. Within the focus of the evaluation:
    - A secure channel cannot be used by another client or another person. Connection parameters are kept secret by the directVPN Zugangssoftware and stored in a non permanent memory of the electronic environment. The protection of those connection parameters is not given if a malicious software copies those data from the memory and uses it for a non intended purpose.

Target of this evaluation (the TOE) is the VPN Software

- **directVPN Zugangssoftware, Version 4.5.50**

1.1 CC Conformance

The assurance requirements are Part 3 [CC] conformant because they are only based upon assurance components in Part 3.

The functional requirements of the TOE are Part 2 [CC] conformant because they are only based upon functional requirements in Part 2.

The selected EAL is EAL1 according to [CC].

2 TOE Description

2.1 Product Type

The directVPN Solution eliminates most of the traditional VPN problems and simplifies VPN configuration. Some of the advantages include:

- Software Network Overlay Architecture—Runs entirely as a software overlay on top of any existing IP-based physical network infrastructure (wired and wireless).
- End-to-end VPN tunnels—Each computer within the VCN Network is considered a VPN endpoint or node. Communications cannot be intercepted even if the corporate network is compromised.
- Domain Name Routing—VPN tunnels can traverse firewalls, private networks, or even multiple private networks that use the same IP address space.
- Dynamic VPN tunnels—All VPN members (nodes) automatically establish their own VPN tunnels. Once you add a member and configure its permissions, it automatically establishes connections with other members in its community.
- Central administration and control with automatic remote policy enforcement—Access control and connectivity based on rules assigned to the user and not to specific systems. Rules are enforced by both local and remote endpoints.
- End-to-end connectivity—Uses the IETF standard for data privacy and authentication from endpoint-to-endpoint. Data is not compromised on the Internet or private networks.
- Cross ISP support—Implementation directVPN Zugangssoftware requires no support or intervention from ISPs. VPN members simply require IP connectivity to the Internet.
- Simple extranet configuration—Extranet partners can be added to the network quickly easily controlled.

2.1.1 Components of the directVPN Software Suite

Other software components, that are not part of the TOE, but the TOE is working with:

- **VCN Community Server**

The VCN Community Server is the main component of the Solution. It is responsible for establishing domains, establishing VCNs, authenticating instances of the directVPN Zugangssoftware and Administrators, and providing information that allows the instances of the directVPN Zugangssoftware to establish secure communications. The instances of the directVPN Zugangssoftware are also called *Member Agents* or—more accurately—*VCN Member Agent*. Depending on the context, this term may also stand for the node itself which runs an instance of the directVPN Zugangssoftware.

2.1.2 Delimitation of the TOE

The directVPN Zugangssoftware (except the underlying operating system WINDOWS) represents the TOE which provides the following capabilities and security functionalities:

The TOE provides the following **security functionalities**:

1. **Security function 1: Key File-Access (Figure 1, (5))**
   - The membership information can be exported encrypted to a key file by the TOE.
   - The key used for encryption is derived by the TOE from the entered password.
   - For importing / exporting membership information from/to a Key File the TOE-User has to provide a key file password (called within this document: “Key File-Password”.
   - The membership information can only be imported if the TOE-User provides the correct password.
   - The TOE visualises unsuccessful authentication attempts occur related to the entry of a password when importing membership information. There is no measure to lock the key file if the number of unsuccessful attempts reaches a fixed number.

2. **Security function 2: Secure Channel(Figure 1, (4))**
   - The TOE (directVPN Zugangssoftware) establishes a secure channel to another directVPN Zugangssoftware, if both directVPN clients joined the same VCN (to decide if a member is active or not is done via a request at the VCN Community Server).
   - The established secure channel is used to exchange the application data (O7) confidential and integer.

The TOE protects

- the application data transmitted via internet between different directVPN Zugangssoftware within the same VCN and
- the membership information within the key file when transported from one directVPN Zugangssoftware to another (e.g. disk, USB stick).

The directVPN Zugangssoftware has the following **capabilities** (not in scope of the evaluation):

- Provides a Graphical User Interface (GUI) for communicating with the VCN Community Server.
- The GUI/CLI prepares the following service requests and submits them to the VCN Community Server:
  - Join Requests
  - Query Requests
  - Connection Requests
  - Leave Requests
  - Change Password Requests
  - Import/Export membership information Requests (stored in so called Key Files)
  - Secure File Sharing Request
  - Displays results of the VCN Community Server processing the service requests.
- Provides secure communications with the VCN Community Server.
- Allows members who have private IP addresses to do host-to-host exchange of encrypted IP packets with the VCN Community Server, which has a public IP address.
- Supports member authentication using Digital Certificates.
- Allows applications (such as telnet, ftp or browser) to establish connections with other active members.
- Downloads changes to the member's User Information File when the member joins the VCN.
- Supports Secure File Sharing between VCN Members
- Provides online user help information (e.g. Help Pages, contact information, etc.).

Delivery Scope of the TOE:

The TOE can be downloaded via Internet or is delivered on CD-ROM as an executable setup file named “dvpnclient.exe”.

The TOE needs the following requirements:

- Physical Location: Any network with public Internet access
- Network Access: Private network or direct Internet connection
- Soft- or hardwarefirewall (to provide attacks from the internet)
- Ports (default, must be allowed by the firewall): TCP: 80, 433, 900, 9001, 9002; UDP: 20202
- Platform(s): PC with 64 MB of RAM (minimum)
- Processor: Intel/AMD 32-bit x86 based PC, 233 MHz or higher
- One of the following operating systems: Windows XP Home Edition, Windows XP Professional, Windows 2000, Windows 98 SE, Window 2000 Advanced Server
- Web Browser compatible to Internet Explorer 5.5 to display Help-pages
- Requires Fixed IP(s): No

2.1.3 Operational modes of the TOE

The following operational modes of the TOE exist:

- „off“ mode: the TOE is not started.
- “connected” mode: the TOE is started, a connection to the VCN is established. In this mode the TOE can provide the security functions SF1 and SF2.
- “disconnected” mode: the TOE is started, but not connected to a VCN. In this mode the TOE can provide the security function SF1.

2.1.4 Ease of use within the directVPN Solution

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

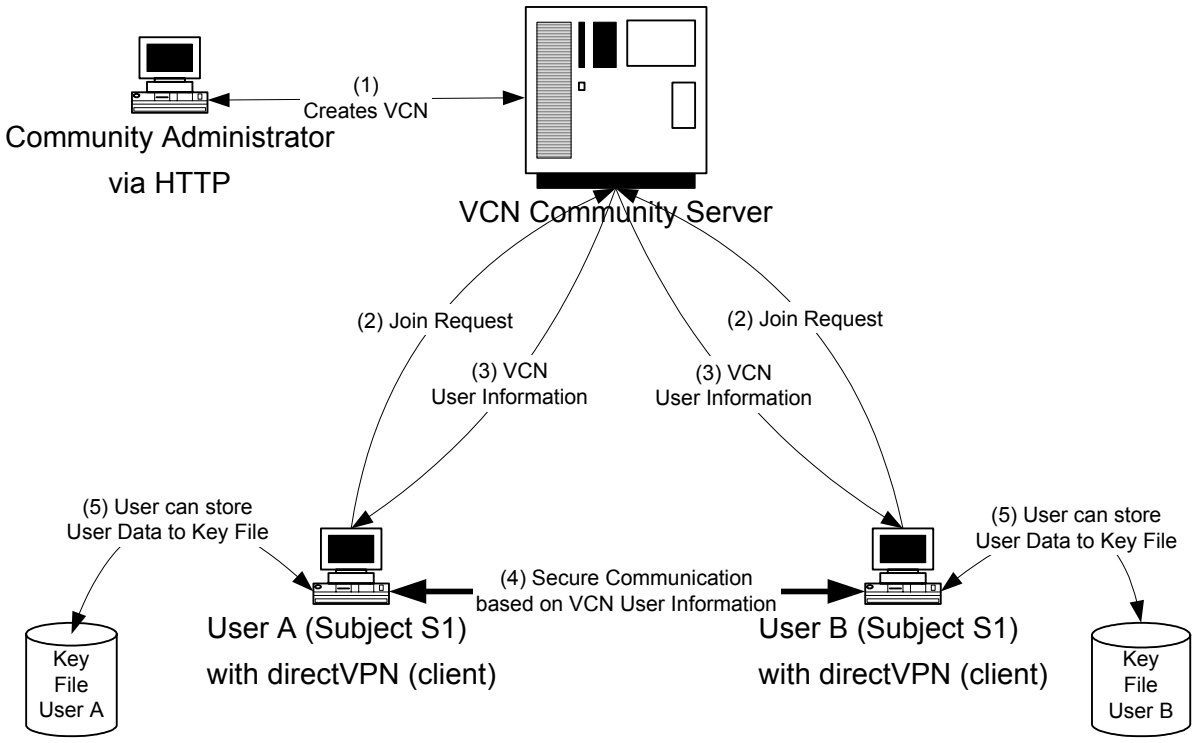

Figure 1 : The TOE within the VCN-Network

In establishing a VCN Network, the future administrator of this VCN network, the so called community administrator, registers at the T-Online International AG the new community and creates (Figure 1, (1)) the VCN within their customer domain, and pre-registers members in the VCNs (so called VCN Members). The community administrator transmits all necessary information to every member using a communication channel he prefers (mail, telephone, etc.). Password information regarding the VCN (VCN password) are transmitted by the community administrator using a communication channel he prefers (telephone, mail etc.).

Each member of a VCN installs the directVPN Zugangssoftware on their computer(s), and then they register in their VCN.

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 (Figure 1, (2)) in a way that ensures that only registered members of a VCN can join the VCN. This is done in the following way: During registration membership information for that VCN are downloaded to the PC 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. Once registered in the VCN, the directVPN Zugangssoftware is ready for use as a participant of that VCN (active member).

When the VCN Community Server joins the member to the VCN, the member becomes an active member of the VCN and gets information about all other active members (Figure 1, (3)). A secure VCN-Connection is visualized by a lock-icon at the lower left border ( ).

An individual who has a member account in multiple VCNs can only be an active member in a single VCN. An active member of a VCN can establish a secure connection with another active member of the same VCN.

Two active VCN members can establish a VCN Connection with each other using any application program that supports communication over the Internet (Figure 1, (4)), or using the VCN Secure File Share. Actually, the secure communication channel is a logical channel. If both clients got a fixed IP address (dialled in via ISDN, modem, DSL, etc), the encrypted data packages from one directVPN Zugangssoftware are routed directly to the other directVPN Zugangssoftware. If not (one or both directVPN Zugangssoftware clients are situated behind a NAT-router), the encrypted data packages from one directVPN Zugangssoftware to the other directVPN Zugangssoftware are routed via the VCN Community Server. The encrypted data can't be read anyway at the VCN Community Server in clear.

An active member can submit a Leave Request to the VCN Community Server to leave their VCN, and when the member leaves the VCN, they become an inactive member of the VCN.

There are three important aspects to remember in regard to members communicating over the VCN network:

- An inactive member cannot be connected to another member (i.e., they are disconnected from the "Private LAN" so they cannot use it).
- An active member of one VCN cannot be connected to an active member of a different VCN (i.e., the "Private LAN" are isolated from each other).
- The VCN Network's traffic is actually transferred over the physical network (i.e., the "Private LAN" that connects members is a concept, not a functional network).

3 TOE Security Environment

3.1 Subjects, Objects and Access Types

3.1.1 Subjects

There are the following types of subjects (which in this case are actors) to be distinguished:

S1 **directVPN Zugangssoftware User**: Person who establishes a **secure channel** from the TOE (directVPN Zugangssoftware) to another directVPN Zugangssoftware within the same VCN

S2 **Community Administrator**—creates and manages VCNs within the domain. Also, creates and manages directVPN Zugangssoftware Users that belong to the VCNs.

S3 **Other person** (neither S1 nor S2).

3.1.2 Objects

O1 Secure channel (regarding integrity and confidentiality) between the TOE and another directVPN Zugangssoftware

O2 Secure channel (regarding integrity and confidentiality) between the TOE and the VCN Community Server

O3 VCN password to access a VCN. Password which must be provided to the TOE for authentication and to access the VCN Community Server.

O4 Admin-password to access an administrator VCN

O5 Membership information. The membership information includes the information necessary to identify to the VCN Community Server as a registered member of the VCN. The membership information can be stored encrypted into a Key File and be imported at the same or another PC using the directVPN Zugangssoftware

O6 Key file password. This password is used to encrypt the Key File which is stored on hard disk.

O7 Application data. Data which are transmitted from the TOE to another VCN Member Agent. The application data are transferred in an encrypted way to keep integer and confidential.

O8 Information about active VCN members. This list represents all other active VCN Member Agents. A VCN connection can be established to all VCN Member Agents listed in here.

3.1.3 Access Types (Operations)

MP Modifying his/her own password (only after entry the old password)

M Manage (create/delete/change)

E Establishing a secure channel

EI Export/Import of membership information to or from a Key File

T Transmit of application data from the TOE to another VCN Member Agent.

VS View/Select

3.1.4 Authorization Concept

An authorization concept for access to the objects defined in chapter 3.1.2 is determined in this chapter. The following table shows the subject types and the permitted operations assigned to them:

	Operations concerning to							
Subject	O1	O2	O3	O4	O5	O6	O7	O8
S1	E	E	MP	-	EI	MP	T	VS
S2	-	-	M	MP	M	-	-	
S3	-	-	-	-	-	-	-	

Table 1: Authorization Concept

- Subject S1:

The subject S1 is authorized to establish (E) a secure channel (O1) to another directVPN Zugangssoftware of the same VCN by selecting (VS) an active VCN Member (using O8). He even may establish (E) a secure channel (O2) to the VCN Community Server. S1 is allowed to change his password (MP) regarding O3 and O6. Furthermore he is allowed to export and import his membership information (O5) to/from a so called Key File, using a special password (O6). S1 can transfer encrypted *application data* from the TOE to another VCN Member Agent.

- Subject S2:

The subject S2 is authorized to manage (M) the VCN-Password (O3) of S1 while administrating a VCN. S2 is authorized to manage (M) membership information (O5) of directVPN Zugangssoftware User (S1). By doing that he sets rights to a person to join a VCN. This management is done using a direct link to the VCN Community Server via a common internet explorer. Furthermore S2 is allowed to change his password (MP).

- Subject S3:

The subject S3 has no authorisation to access any object defined in chapter 3.1.2.

3.2 Assumptions

A.ADMIN
It must be assumed that competent and trustworthy community administrator 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* are 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. These information are 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 (O8).

3.3 Threats

The assumed potential attacker attacks the application data transported via internet and the membership information stored in the key file. He uses only public available information to perform attacks.

T.MOD_AD
An unauthorized person (any other person than subject S1) could modify the *application data* that are part of the information flow between TOE and other directVPN Zugangssoftware.

T.MOD_MI
An unauthorized person (any other person than subject S1) could modify the *membership information* during the transport of the key file to another client.

T.SPY_AD
An unauthorized person (any other person than subject S1) could get knowledge of the *application data* that are part of the information flow between TOE and other directVPN Zugangssoftware via internet.

T.SPY_MI
An unauthorized person (any other person than subject S1) could get knowledge of the *membership information* during the transport of the key file to another client.

4 Security objectives

4.1 Security objectives for the TOE

O.DISCLOSURE
The TOE prevents the disclosure of *application data* during data transfer from TOE to another directVPN Zugangssoftware.

O.INTEGRITY
The TOE applies integrity protection to all *application data* transferred from TOE to another directVPN Zugangssoftware.

O.SECURE_MI_IMPORT_FROM_KEYFILE
The TOE supports the secure import of *membership information* from the key file and ensures the confidentiality and data integrity of the *membership information* within that channel from the key file to the directVPN Zugangssoftware.

O.ACCESS
Only authorized user can access (import or export) the *membership information* which are stored (in a confidential and integer way) in the Key File.

4.2 Security objectives for the environment

OE.ADMIN
Competent, trustworthy and authorized System Administrators (Community Administrator) are assigned as required.

OE.MEMBERSHIP_INFORMATION
The *membership information* transmitted to the directVPN Zugangssoftware when initiating a connection were created by community administrators.

OE.AUTHORISATION
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)**.** Before establishing a connection to another directVPN Zugangssoftware the VCN member must be authenticated by the VCN Community Server by providing the right VCN Password. The VCN Community Server ensures that only authorized VCN Member Agents are listed in O8.[1]

OE.SECURE_MI_EXPORT_TO_MEMBERAGENT
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.

OE.AVAILABLE
Internet or other required public network connections are available to the TSF when required. OE.AVAILABLE is defined as non-IT and is not gained by any security functional requirement.

OE.PROTECTION
The directVPN Zugangssoftware PC is sufficiently protected against malicious code or direct attacks using virus scanning tools and firewalls. OE.PROTECTION is defined as non-IT and is not gained by any security functional requirement.

5 IT Security Requirements

This chapter describes the functionality requirements and the assurance requirements that the TOE fulfils.

The *Security Functional Requirements* includes only components from Part 2 of the CC.

The *Security Assurance Requirements* includes only components from Part 3 of the CC.

[1] O8 lists all other active VCN Member Agents

5.1 TOE Security Functional Requirements

No	ID	**Class**/Component	Dependency
	FCS	**Cryptographic support**	
1	FCS_COP.1	Cryptographic operation	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2
2	FCS_CKM.1	Cryptographic operation	FCS_COP.1 FCS_CKM.4 FMT_MSA.2
	FDP	**User data protection**	
3	FDP_ACC.1	Subset access control	FDP_ACF.1
4	FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3
5	FDP_ITC.1	Import of user data without security attributes	FDP_ACC.1 FMT_MSA.3
6	FDP_ETC.1	Export of user data without security attributes	FDP_ACC.1
	FIA	**Identification and authentication**	
7	FIA_SOS.1	Verification of secrets	No.
	FTP	**Trusted Path/ Channel**	
8	FTP_ITC.1	Inter-TSF trusted channel	No

Table 2: Security Functional Requirements

In the following chapters the operations carried out within the TOE-security requirements are placed in fat letters to clearly identify them. The references are placed inside square brackets.

FCS_COP.1 - Cryptographic operations

FCS_COP.1	The TSF shall perform ***an encryption and decryption*** in accordance with a specified cryptographic algorithm ***not known*** and cryptographic key sizes ***not known*** that meet the following: ***not applicable***.
Remark:	The cryptographic algorithm and the key size are not given because these information are

confidential. These information are not necessary to explain within EAL 1.

FCS_CKM.1 - Cryptographic key generation

FCS_CKM.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm ***not known*** and specified cryptographic key sizes ***not known*** that meet the following: ***not applicable***.
Remark:	FCS_CKM.1 derives the key for encrypting and decrypting from the entered keyfile password. The cryptographic algorithm for the key generation and the key size are not given because these information are confidential. These information are not necessary to explain within EAL 1.

FDP_ACC.1 - Subset access control

FDP_ACC.1.1	The TSF shall enforce the Access Control-SFP (AC-SFP) on the following: subject S1, objects O5 and O6, operations EI and MP.
Remark:	S1 is only authorized to import or export (EI) membership information to/from the key file on hard disk of his PC. S1 is allowed to change (MP) his password regarding O6.

FDP_ACF.1 - Security attribute based access control

FDP_ACF.1.1	The TSF shall enforce the ***AC-SFP*** to objects based on ***password***.
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Subject S1

To import or export the membership information (O5) from/to the key file (in a confidential and integer way) on the hard disk of his PC subject S1 has to enter his Key file Password (O6).

Subject S1 could modify the Key file Password (O6) only after entry of the old password.

FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***no assignment***.
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the ***no assignment***.

FDP_ITC - Import from Outside TSF Control

FDP_ITC.1	Import of User Data without Security Attributes
FDP_ITC.1.1	The TSF shall enforce the ***Access Control-SFP (AC-SFP)*** when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: ***the membership information may only be imported if they are integer and could be decrypted in a correct way.***
Remark:	The term ‘user data’ means in this context membership information for the TOE.

FDP_ETC - Export to Outside TSF Control

FDP_ETC.1	Export of User Data without Security Attributes
FDP_ETC.1.1	The TSF shall enforce the ***Access Control-SFP (AC-SFP)*** when exporting user data, controlled under the SFP, outside of the TSC.
FDP_ETC.1.2	The TSF shall export the user data without the user data’s associated security attributes.
Remark:	The term ‘user data’ means in this context membership information for the TOE.

FIA – Identification and authorisation

FIA_SOS.1 - Verification of secrets

FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet ***keyfile password length must be 8 characters or greater***.

FTP – Trusted path/ channel

FTP_ITC.1 – Inter TSF trusted channel

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product[2] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit ***the TSF, the remote trusted IT product*** to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for ***the confidential and integer transport of application data (O7) to another TOE***.

5.2 TOE Security Assurance Requirements

The TOE is to fulfil the assurance requirements according to class ASE (to examine the existing security targets) and evaluation level EAL1. All these requirements are listed in the table shown below.

Assurance class	ID	Assurance components
Security Target Evaluation	ASE_DES.1	TOE description
	ASE_ENV.1	Security environment
	ASE_INT.1	ST Introduction
	ASE_OBJ.1	Security objectives
	ASE_PPC.1	PP claims
	ASE_REQ.1	IT-security requirements
	ASE_SRE.1	Explicitly stated IT-security requirements
	ASE_TSS.1	TOE summary specification
Configuration management	ACM_CAP.1	Version numbers

[2] directVPN Zugangssoftware

Assurance class	ID	Assurance components
Delivery and operation	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	-	-
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability assessment	-	-

Table 3: Assurance requirements (ASE and EAL1)

5.3 Security Requirements for the environment

No	ID	**Class**/Component	Dependency
	FTP	**Trusted Path/ Channel**	
1	FTP_ITC.1+1	Inter-TSF trusted channel	No
	FDP	**User data protection**	
2	FDP_ACC.2	Complete access control	FDP_ACF.1
3	FDP_ACF.1+1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3
	FIA	**Identification and authentication**	
4	FIA_UAU.2	User authentication before any action	FIA_UID.1
5	FIA_UAU.1	Timing of authentication	FIA_UID.1
6	FIA_UID.2	User identification before any action	no
7	FIA_UID.1	Timing of identification	no

Table 4: Security Functional Requirements for the environment

FTP_ITC.1 +1 – Inter TSF trusted channel

FTP_ITC.1.1+1	The TSF shall provide a communication channel between itself and a remote trusted IT product[3] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2+1	The TSF shall permit ***the remote trusted IT product: directVPN Zugangssoftware*** to initiate communication via the trusted channel.
FTP_ITC.1.3+1	The TSF shall initiate communication via the trusted channel for: • ***The transport of membership information (O5) between the directVPN Zugangssoftware and the VCN Community Server*** • ***The transport of the VCN-password (O3)*** • ***Information about active VCN members (O8)***

FIA – Identification and authorisation

FIA_UAU.2 - User authentication before any action

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Remark:	The VCN Community Server asks for user authentication (community administrator) before it is possible to manage the VCN-Domain (incl. membership information). The community administrator has to authenticate himself via internet (Figure 1, (1)).

FIA_UID.2 - User identification before any action

FIA_UID.2.1	The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
Remark:	The VCN Community Server asks for user identification (community administrator) before it is

[3] Channel between VCN Community Server and directVPN Zugangssoftware

possible to manage the VCN-Domain (incl. membership information). The community administrator has to identify himself via internet (Figure 1, (1)).

FIA_UAU.1 - Timing of authentication

FIA_UAU.1.1	The TSF shall allow [**the Export of membership information, the Deleting of membership information, the Logging of actions, the Test of connectivity, the Activating/Deactivating of SecureFileShare**] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Remark:	The TOE User has to authenticate himself to the VCN Community Server when initiating a first connection to the VCN. (“Join Request”, Figure 1, (2))

FIA_UID.1 - Timing of identification

FIA_UID.1.1	The TSF shall allow **[the Export of membership information, the Deleting of membership information, the Logging of actions, the Test of connectivity, the Activating/Deactivating of SecureFileShare**] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Remark:	The TOE User has to identify himself to the VCN Community Server when initiating a first connection to the VCN (“Join Request”, Figure 1, (2)).

FDP - User data protection

FDP_ACC.2 - Complete access control

FDP_ACC.2.1	The TSF shall enforce the **Access Control-SFP (AC-SFP-ENV) on the following subjects S1 and S2, and objects O1, O2, O3 and O4**, and all

	operations among subjects and objects covered by the SFP.
FDP_ACC.2.2	The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

FDP_ACF.1 +1 - Security attribute based access control

FDP_ACF.1.1 +1	The TSF shall enforce the ***AC-SFP-ENV*** to objects based on ***membership information and password***.
FDP_ACF.1.2+1	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Subject S1

The subject S1 is authorized to establish a secure channel to another VCN-Member-Agent after providing the correct membership information (O5) and the correct VCN password to the VCN Community Server.

The subject S1 is authorized to establish a secure channel to VCN Community Server after providing the correct membership information (O5) and the correct VCN password to the VCN Community Server.

The subject S1 is able to modify his/ her VCN-password (object of type O3) after entry of the old valid password.

Subject S2

The subject S2 is able to modify his/ her Admin-password (object of type O4) after entry of the old valid password.

The subject S2 is authorized to manage (M) the VCN-Password (O3) of S1 while administrating a VCN.

The subject S2 can manage the membership information (O5) after Logon at the VCN Community Server.

FDP_ACF.1.3 +1	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***no assignment***.
FDP_ACF.1.4 +1	The TSF shall explicitly deny access of subjects to objects based on the ***no assignment***.

6 TOE Summary Specification

6.1 TOE Security Functions

6.1.1 Security function 1: Key File-Access (SF1)

The membership information can be exported encrypted and integrity protected to a key file by the TOE.

The SF1 allows the subject S1 (i.e. TOE-User) to enter the “Key File Password” (O6). The entered password is not displayed on the screen. The password is used as key for encrypting (in case of membership information export to Key File) and decrypting (in case of membership information import from Key File) the Key File.

The password must be set initially when creating a new Key File. The password can only be modified after entering the old password.

The TOE provides an authentication of S1 when importing the membership information (O5) from a Key File in a confidential and integer way. If the entered password is correct, the Key File can be decrypted and the TOE allows the import of membership information from the Key File. If the entered password is incorrect, the TOE visualizes the wrong attempt.

There is no mechanism to lock the Key File if the number of consecutively failed authentication attempts with ”Key File Password” (O6) exceeds a fixed number.

Remark: The TOE forces no password-requirements regarding quality of the Key file Password. The TOE uses a basic password policy regarding the password length (8 characters). The Key File Password is never stored permanently as plaintext.

6.1.2 Security function 2: Secure Channel (SF2)

The TOE provides a secure encrypted channel to communicate with another directVPN Zugangssoftware which is a member of the same VCN. Both sides of a channel (resp. both VCN Members) are assured identified by their personal membership information (O5).

The secure channel is used to exchange the application data (O7) confidential and integer.

A secure channel can be initialized by both S1 (using the TOE) and every other active member of the same VCN.

6.1.3 Strength of Functions Claim

No claim is required because AVA_SOF.1 is not part of EAL1.

6.2 Assurance Measures

The TOE is to fulfill the assurance requirements of assessment class ASE and of evaluation level EAL1. The present document "Security Targets" serves to fulfill the requirements according to ASE. Besides the TOE (according to ATE_IND.1), the manufacturer will provide

the following additional documents within the frame of the evaluation, to evidently prove the fulfilling of the requirements according to EAL1:

- Configuration management documentation (acc. to ACM_CAP.1)
- Delivery and operational documentation (according to ADO_IGS.1)
- Development documentation (according to ADV_FSP.1 and ADV_RCR.1)
- Guidance documents (according to AGD_ADM.1 and AGD_USR.1)

The assignment of the assurance measures to the assurance requirements is shown in chapter 8.7.4.

7 PP Claims

No reference is made to a protection profile.

8 Rationale

8.1 Security objectives Rationale

This section describes the suitability of the TOE's security features to counter all assumed threats. An easy mapping between the threats and the security objectives is done in the following table:

Threats	Security objectives for the TOE and the environment
T.MOD_AD	**O.Integrity**
T.MOD_MI	**O.Secure_MI_Import_FROM_KEYFILE,** **OE.SECURE_MI_EXPORT_TO_MEMBERAGENT,** **OE.MEMBERSHIP_INFORMATION**
T.Spy_AD	**O.Disclosure**
T.Spy_MI	**O.Access**

Table 5: Mapping between threats and security objectives

T.MOD_AD

The threat T.MOD_AD will be covered by the security objective O.Integrity. It keeps the integrity of the *Application data* transferred between the TOE and another VCN entity.

T.MOD_MI

The threat T.MOD_MI is covered by the security objective O.SECURE_MI_IMPORT_FROM_KEYFILE, OE.MEMBERSHIP_INFORMATION and OE.SECURE_MI_EXPORT_TO_MEMBERAGENT.

O.SECURE_MI_IMPORT_FROM_KEYFILE ensures that the TOE has the capability to provide a secure import of membership information from the key file.

OE.SECURE_MI_EXPORT_TO_MEMBERAGENT ensures that the membership information are exported in a secure way from VCN Community Server to the directVPN Zugangssoftware.

OE.Membership_Information ensures that the VCN Community Server ensures that only authorized VCN Member Agents can establish a secure channel within in a VCN**.**

T.SPY_AD

The threat T.Spy is covered by the security objective O.Disclosure, which provides the confidentiality of the *application data* during transmission.

T.SPY_MI

This threat is covered by the security objective O.Access. O.Access ensures that only authorized users can access (import or export) the *membership information.*

8.2 Coverage of the assumptions

Assumptions	Security objectives for the environment
A.ADMIN	OE.ADMIN
A.MEMBERSHIP_INFORMATION	OE.MEMBERSHIP_INFORMATION
A.SECURE_MI_EXPORT	OE.SECURE_MI_EXPORT_TO_MEMBERAGENT
A.AVAILABLE	OE.AVAILABLE
A.AUTHORISATION	OE.AUTHORISATION
A.PROTECTION	OE.PROTECTION

Table 6: Assignment: assumptions – security objectives for the environment

8.3 Security Requirements Rationale

This chapter proves that the quantity of security requirements (TOE and environment) is suited to fulfil the security objectives described in chapter 4 and that it can be traced back to the security objectives. The security requirements for the environment are placed in fat

letters. All security objectives of the TOE are fulfilled. At least one security objective exists for each security requirement.

	O.DISCLOSURE	O.INTEGRITY	O.SECURE_MI_IMPORT_FROM_KEYFILE	O.ACCESS	OE.MEMBERSHIP_INFORMATION	OE.SECURE_MI_EXPORT_TO_MEMBERAGENT	OE.AUTHORISATION
FCS							
FCS_COP.1				X			
FCS_CKM.1				X			
FDP							
FDP_ACC.1				X			
FDP_ACF.1				X			
FDP_ACC.2					X		
FDP_ACF.1+1					X		
FDP_ITC.1			X				
FDP_ETC.1				X			
FIA							
FIA_SOS.1				X			
FIA_UAU.2					X		
FIA_UAU.1							X
FIA_UID.2					X		
FIA_UID.1							X
FTP							
FTP_ITC.1	X	X					
FTP_ITC.1+1						X	

Table 7: Assignment: security requirements – security objectives for TOE and IT environment

O.DISCLOSURE

The security objective O.Disclosure is gained by FTP_ITC.1 because the trusted channel guarantees the confidentially of the transmitted *application data*.

O.INTEGRITY

The security objective O.Integrity is gained by FTP_ITC.1 because the Inter-TSF trusted channel provides the protection of the channel data from modification or disclosure.

O.SECURE_MI_IMPORT_FROM_KEYFILE

The security objective is gained by FDP_ITC.1. FDP_ITC.1 ensures the integrity protection and data disclosure when importing *membership information*.

O.ACCESS

The security objective O.ACCESS is gained by FDP_ACC.1, FDP_ACF.1, FCS_CKM.1, FDP_ETC.1, FIA_SOS.1 and FCS_COP.1.

From the entered password the TOE derives a symmetric key to encrypt or decrypt the membership information (FCS_CKM.1 and FCS_COP.1). So there is an implicit access control provided by FDP_ACC.1, FDP_ACF.1 and FDP_ETC.1; only an authenticated user could access to the membership information. FIA_SOS.1 assures that the key file password length must be 8 or greater.

OE.MEMBERSHIP_INFORMATION

The security objective OE.MEMBERSHIP_INFORMATION is gained by FDP_ACC.2, FDP_ACF.1+1, FIA_UAU.2 and FIA_UID.2.

The VCN Community Server provides the necessary I&A functionality realized by FIA_UAU.2 and FIA_UID.2 and ensures that only authorized VCN Member Agents can establish a secure channel within a VCN. FDP_ACC.2 ensures the enforcement of the Access Control-SFP (AC-SFP-ENV) on the subjects S1 and S2, the objects O1, O2, O3 and O4, and all operations among subjects and objects covered by the SFP. FDP_ACF.1+1 provides the necessary security attribute based access control (rules) on the subjects S1 and S2 regarding the membership information.

OE.SECURE_MI_EXPORT_TO_MEMBERAGENT

The security objective OE.SECURE_MI_EXPORT_TO_MEMBERAGENT is gained by FTP_ITC.1+1. This trusted channel covers all operations within the VCN Community Server necessary to establish a secure channel to export *membership information*.

OE.AUTHORISATION

To connect a VCN a Member Agent has to identify and authenticate himself to the VCN Community Server. The VCN Community Server provides the necessary I&A functionality realized by FIA_UAU.1 and FIA_UID.1. Only identified and authenticated VCN Member Agents are listed in O8 by the VCN Community Server.

8.4 Fulfilling all dependencies of the security requirements of the TOE

The following table shows that all dependencies of the functional IT-security requirements of the TOE are fulfilled:

No.	ID	**Class**/Component	Dependency	Dependency met by No.
	FDP	**User data protection**		
1.	FDP_ACC.2	Complete access control	FDP_ACF.1	2.
2.	FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	1. 6.
3.	FDP_ITC.1	Import of user data without security attributes	FDP_ACC.1 FMT_MSA.3	1. 6.
4.	FDP_ETC.1	Export of user data without security attributes	FDP_ACC.1	1.
	FIA	**Identification and authentication**		
5.	FIA_SOS.1	Verification of secrets	No.	
	FMT	**Security Management**		
6.	FMT_MSA.3 Static attribute initialization The dependency FMT_MSA.3 (from FDP_ACF.1) is formal not given. The TOE doesn't offer the possibility to set the given security attributes. The dependency FMT_MSA.3 (from FDP_ITC.1) is formal not given. The TOE doesn't offer the possibility to set the given security attributes.			
7.	FMT_MSA.2 Secure security attributes The dependency FMT_MSA.2 is not given because the TOE forces no password-requirements regarding quality of the Key file password.			
	FTP	**Trusted Path/ Channel**		
8.	FTP_ITC.1	Inter TSF trusted channel	No	-
	FCS	**Cryptographic operation**		
9.	FCS_COP.1	Cryptographic operation	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	10. 11. 7.
10.	FCS_CKM.1	Cryptographic key generation	FCS_COP.1	9.

No.	ID	**Class**/Component	Dependency	Dependency met by No.
			FCS_CKM.4 FMT_MSA.2	11. 7.
11.	FCS_CKM.4 Cryptographic key destruction: The dependency FCS_CKM.4 (from FCS_COP.1 and FCS_CKM.1) is not fulfilled, because the way of destruction is not known (within an EAL1 evaluation this information is not needed).			

Table 8: Dependencies of the functional IT-security requirements of the TOE

8.5 Fulfilling all dependencies of security requirements of the environment

The following table shows that all dependencies of the functional IT-security requirements of the environment are fulfilled:

No.	ID	**Class**/Component	Dependency	Dependency met by No.
	FIA	**Identification and authentication**		
1.	FIA_UAU.2	User authentication before any action	FIA_UID.1	3.
2.	FIA_UAU.1	Timing of authentication	FIA_UID.1	4.
3.	FIA_UID.2	User identification before any action	no	-
4.	FIA_UID.1	Timing of identification	no	-
	FDP	**User data protection**		
5.	FDP_ACC.2	Complete access control	FDP_ACF.1	6.
6.	FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	5. 7.
	FMT	**Security Management**		
7.	FMT_MSA.3 Static attribute initialization The dependency FMT_MSA.3 (from FDP_ACF.1) is not fulfilled because dependencies of requirements of the environment are not taken into consideration.			
	FTP	**Trusted Path/ Channel**		
8.	FTP_ITC.1+1	Inter-TSF trusted channel	no	-

Table 9: Dependencies of the functional IT-security requirements of the environment

8.6 Assurance Requirements Rationale

To select the assurance class ASE is obligatory for the evaluation of a concrete TOE.

The selection of the EAL level will prove to be suitable, if the rating is appropriate to the assurance resulting here from. The selected level EAL1 ensures a minimum extent of confidence into the security examined by an independent authority. The evaluator checks the TSF on the base of independent testing. In view of the operational environment, no explicit attack potential for exploiting the weaknesses of the TOE is utilized. Considering the fact that no SOF-strength is postulated, it is justified to have selected EAL1.

8.7 TOE Summary Specification Rationale

In this chapter it is shown that the security functions are suited to fulfil the security requirements. It is demonstrated that at least one security function meets each security requirement. Furthermore it is shown that all security functions are needed and that they form an integrated unity to meet the security requirements.

8.7.1 Fulfilling the security functional requirements

	SF1	SF2
FCS		
FCS_COP.1	X	
FCS_CKM.1	X	
FDP		
FDP_ACC.1	X	
FDP_ACF.1	X	
FDP_ITC.1	X	
FDP_ETC.1	X	
FIA		
FIA_SOS.1	X	
FTP		
FTP_ITC.1		X

Table 10: Assignment: security requirements – security functions

FCS_COP.1

FCS_COP.1 is realized by SF1. SF1 uses a symmetric algorithm to encrypt and decrypt the *membership information* stored in the key file.

FCS_CKM.1

FCS_CKM.1 is realized by SF1. SF1 derives the key for encrypting and decrypting from the entered key file password.

FDP_ACC.1

FDP_ACC.1 is realized by SF1. SF1 provides the access control of the TOE.

FDP_ACF.1

FDP_ACF.1 is realized by SF1. SF1 provides the access control of the TOE.

FDP_ITC.1

FDP_ITC.1 is realized by SF1. SF1 ensures the secure import of *membership information* from the key file.

FDP_ETC.1

FDP_ETC.1 is realized by SF1. SF1 ensures the secure export of *membership information* to the key file.

FIA_SOS.1

FIA_SOS.1 is realized by SF1. SF1 ensures that the length of the key file Password is 8 or greater.

FTP_ITC.1

FTP_ITC.1 is realized by SF2. SF2 ensures a trusted channel between the TOE and another directVPN Zugangssoftware.

8.7.2 Consistency of the Strength of Function Claims

Not required because AVA_SOF.1 is not part of EAL1, i.e. no strength of function claim is done.

8.7.3 Analysis of the Combination of the Security Functions

No security functions are combined.

8.7.4 Assurance Measures Rationale

The assurance measures taken are described in chapter 6.2. In the following these measures are assigned to the requirements, as stipulated EAL1.

Assurance class		
	Assurance component	Measures taken by the manufacturer
Evaluation of the security targets		
	TOE-description	Security targets (this document)
	Security environment	
	ST Introduction	
	Security objectives	
	PP claims	
	IT-security requirements	
	Explicitly described IT-security requirements	
	TOE summary specification	
Configuration management		
	CM capabilities	A unique reference is required to ensure that there is no ambiguity in terms of which instance of the TOE is being evaluated.
Delivery and operation		
	Installation, generation and start-up procedures	The delivery and installation procedures are described in detail in separate documents. These include descriptions of how the security is maintained throughout these procedures.

Assurance class		
	Assurance component	Measures taken by the manufacturer
Development		
	Informal functional specification	Functional specification Assignment description By means of the development documents the manufacturer provides an exact description of the implementation of the security requirements resulting from the security targets. The compliance of this description with the various degrees of detail content given in each of these documents is ensured.
	Informal correspondence demonstration	
Manuals		
	Administrator guidance	Operational documentation The TOE is delivered together with a detailed system administrator and user documentation
	User guidance	
Testing		
	Independent testing – sample	The manufacturer provides the testing agency with the TOE for their independent tests.

Table 11: Assurance measures

8.8 PP Claims Rationale

Not required, as there is no reference to a PP.

9 Abbreviations

CLI	Command Line Interface
DNS	Domain Name Server
FTP	File Transfer Protocol
GUI	Graphical User Interface
IETF	Internet Engineering Task Force
ISP	Internet Service Provider
LAN	Local Area Network
VCN	Virtual Community Network
VDN™	Virtual Domain Network™
VPN	Virtual Private Network
WAN	Wide Area Network

9.1 Criteria

CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FSP	Informal Functional Specification
OR	Observation Report
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(I)	TOE Security Functions (Interface)
TSS	TOE Summary Specification

9.2 References

[CC] ISO/IEC 15408, Information technology — Security techniques — Evaluation criteria for IT security —, First edition 1999-12-01.

1. ISO/IEC 15408-1:1999(E), Part 1: Introduction and general model.
2. ISO/IEC 15408-2:1999(E), Part 2: Security functional requirements.
3. ISO/IEC 15408-3:1999(E), Part 3: Security assurance requirements.

10 Glossary

Application Data	So called data which are transferred from a computer using the TOE to another VCN Member Agent. The *application data* are transferred in an encrypted way.
Community Administrator	Administrator of a VCN network, which registers the new community at the T-Online International AG, creates the VCN within their Customer Domain and pre-registers members in the VCNs.
directVPN Zugangssoftware PC	A personal computer on which the directVPN Zugangssoftware is running.
Key File	The *membership information* can be exported encrypted to a *key file* to be transferred to another client. The Key File is encrypted by the *Key File-Password*.
Key File-Password	See *Key File*
Membership Information	The *membership information* includes the information necessary to identify to the VCN Community Server as a registered member of the VCN.
User Information File	File that contains the *membership information* for each of the member's VCNs, the computer port setting that the individual uses with the directVPN Zugangssoftware, and other user specific information.
VCN Member Agent	The instances of the directVPN Zugangssoftware are also called *Member Agents* or—more accurately—*VCN Member Agent*. Depending on the context, this term may also stand for the node itself

which runs an instance of the directVPN Zugangssoftware.