Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2009/01

BULL TrustWay VPN Line :

- TVPN v4.05.02
- TCRX/TCRX2 v4.05.01

Paris, 2nd of April 2009

Courtesy Translation

SÉCURITÉ CERTIFICATION

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.
Certification does not, however, constitute a recommendation product from DCSSI (Central Directorate for Information Systems Security), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

Secrétariat Général de la Défense Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.dcssi@sgdn.gouv.fr

Certification report reference

DCSSI-2009/01

Product name

BULL TrustWay VPN Line :
- TVPN v4.05.02
- TCRX/TCRX2 v4.05.01

Product reference

v4.05.02 / b205 pour TVPN
v4.05.01 / c020 pour TCRX/TCRX2

Protection profile conformity

None

Evaluation criteria and version

Common Criteria version 2.3
compliant with ISO 15408:2005

Evaluation level

EAL 2 augmented

ADV_HLD.2, ADV_IMP.1*, ADV_LLD.1*, ALC_DVS.1, ALC_FLR.3, ALC_TAT.1*, AVA_MSU.1, AVA_VLA.2

***applied to FCS requirements**

Developer(s)

Bull SAS
Rue Jean Jaurès – BP 68, 78340 Les Clayes sous Bois, France

Sponsor

Direction Générale de la Gendarmerie Nationale
1, bd Théophile Sueur, 93110 Rosny sous Bois, France

Evaluation facility

Oppida
4-6 avenue du vieil étang, Bâtiment B, 78180 Montigny le Bretonneux, France
Tél : +33 (0)1 30 14 19 00, mél : cesti@oppida.fr

Recognition arrangements

CCRA **SOG-IS**

IT Security Certified

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the principals desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.

Content

1. The product

1.1. Presentation of the product

The evaluated product consists of Bull's TrustWay VPN Line developed by Bull SAS:

- TVPN appliance (Trustway Virtual Private Network) version 4.05.02,
- TCRX appliance (Trustway *Chiffreur Routeur d'eXtrémité*) version 4.05.01,
- TCRX2 appliance (2nd model of TCRX) version 4.05.01.

These appliances are used to link together internal networks to be protected through an external unprotected network. As for, they allow to setting up virtual private networks (VPN) through public networks such as Internet, in order to preserve confidentiality and integrity of data exchanged between remote systems.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.

The certified version of the product can be identified by the following elements:

- for TVPN appliance :
  - TVPN software, version 4.05.02 ;
  - PCA3 card, version 76677843-309 A, firmware v5.5 and its embedded software b205 ;
- for TCRX appliance :
  - TCRX appliance, version 4.05.01 ;
  - Cryptographic card 76679897-106A comprising a cryptographic processor Altera EP1C20F324C8N and its embedded software c020 ;
- For TCRX2 appliance :
  - TCRX software, version 4.05.01 ;
  - Cryptographic card 76680490-105A comprising a cryptographic processor Altera EP1C20F324C8N and its embedded software c020.

These versions can be checked through the administration station TDM (see §1.2.3).

1.2.2. Security services

The product provides mainly the following security services:

- confidentiality and integrity of exchanged data in tunnel mode ;
- no clear flows written on non volatile memory;
- confidentiality and integrity of administration dialogs;
- confidentiality and integrity of configurations;
- warning and destruction of frames in case of data that cannot be authenticated;
- integrity of the software;
- disabling the transmission of non encrypted data;
- control of correspondents authorized to communicate with one another;
- ports filtering;
- addresses filtering;
- anti-replay mechanism for administration flows;
- key management;
- configurations management;
- warnings and supervising.

1.2.3. Architecture

The hardware architecture of the product is:

- for TVPN appliance:
  - one mother card ASROCK I775 GV s775 FSB800 ;
  - one Intel Celeron D 331 2.66Ghz s775 processor ;
  - one 160go PATA Maxtor 8M hard disk ;
  - one 512 Mo memory of RAM 400Mhz CL3 ;
  - one PCA3 card, version 76677843-309A, firmware v5.5, and its embedded software b205 developed by BULL, and performing cryptographic operations ;
  - two Ethernet interfaces ;
  - leds to indicate the chassis activity ;
  - one serial port (used for local administration) ;
  - one power supply ;
- for TCRX appliance:
  - one Intel EGLXT973QCA3V network processor ;
  - one cryptographic card 76679897-106A comprising a cryptographic processor Altera EP1C20F324C8N and its embedded software c020;
  - two Ethernet interfaces ;
  - leds to indicate the chassis activity ;
  - one serial port (used for local administration) ;
- for TCRX2 appliance:
  - one Intel EGLXT973QCA3V network processor ;
  - one cryptographic card 76679897-106A comprising a cryptographic processor Altera EP1C20F324C8N and its embedded software c020;
  - two Ethernet interfaces ;
  - leds to indicate the chassis activity ;
  - one serial port (used for local administration) ;
  - one power supply integrated in the chassis.

The software architecture of the product is:

- for TVPN appliance:
    - one TVPN software, version 4.05.02;
    - one b205 software;
    - one Linux operating system (Linux kernel 2.4.24) ;
    - one Netfilter tool (included in Linux) ;
    - one Tripwire software (version 1.2.2) ;
    - one local administration software module;
- for TCRX/TCRX2 appliances:
    - one TCRX software, version 4.05.01;
    - one c020 software;
    - one Linux operating system (Linux kernel 2.4.24) ;
    - one Netfilter tool (included in Linux) ;
    - one Tripwire software (version 1.2.2) ;
    - one local administration software module;

Locally, the product in linked to an external terminal (SafePad) that is necessary for the authentication of the administration and for the loading of initial keys.

The product is used inside a tipical architecture as drawn here after:

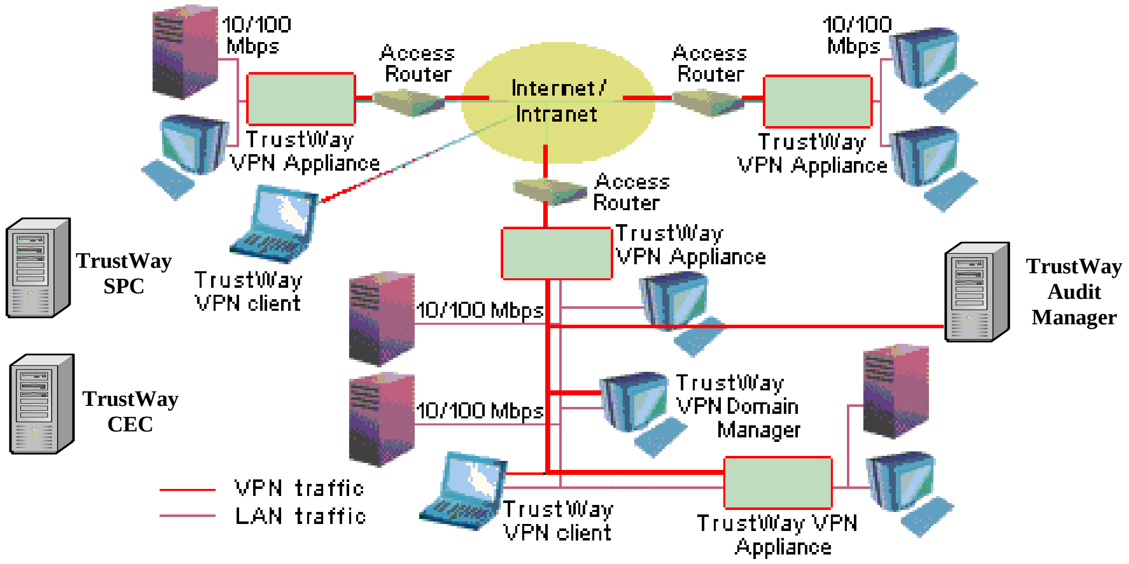

Figure 1 – Architecture d'utilisation

On this picture, we can see different optional modules which are out of the scope of the evaluation:

- VPN client software ;
- personalisation station (SPC) ;
- key generation center (CEC) ;
- administration station Trustway VPN Domain Manager (TDM)
- auditing station Trustway Audit Manager (TAM) ;
- access router.

The TDM offers the possibility to declare complementary servers which may be inserted in the network architecture of the product:

- syslog server which is to receive syslog messages sent by the product;
- snmp supervior server which is to receive snmp trpas sent by the product.

These equipments are out of the scope of the evaluation (and they are not represented on the previous picture).

The various functionalities of these equipments are described in the security target [ST] as well as in the administration guides (see [GUIDES]).

1.2.4. Life cycle

The product has been developed on the following site:

Bull SAS - Les Clayes sous Bois

Rue Jean Jaurès – BP 68,
78340 Les Clayes sous Bois,
France

It has then been integrated and finalised on the following site:

Bull BILS - Angers

357, avenue Patton
49008 Angers Cedex 01
France

There is no user role for the security functions of the product.

1.2.5. Evaluated configuration

The evaluated product comprises the following configurations:

- the TVPN/TCRX softwares ;
- the b205/c020 softwares of the cryptographic card ;
- the software part implementing the communication protocol between the product and the administration station ;
- the software module for local administration.

The following elements are also installed on the product but are out of the scope of the evaluation:

- Linux operating system, including Netfilter tool ;
- Tripwire software.

The following elements are out of the product and are out of the scope of the evaluation, but they are necessary for the product to work:

- one external terminal (SafePad) needed for the authentication of the administrator and for the loading of initial keys ;
- one administration station (TDM);
- one auditing stations (TAM).

Though the product supplies four modes (drop, forward, IPSEC-transport, IPSEC-tunnel), only the latter mode is under the perimeter of the evaluation.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC], with the Common Evaluation Methodology [CEM].

2.2. Evaluation work

The evaluation relies on the evaluation results of the BULL Trustway VPN Appliance v3.01.06 product certified by DCSSI (see [2004/30]).

The evaluation technical report [ETR], delivered to DCSSI on 11 march 2009, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are “**pass**”.

2.3. Cryptographic mechanisms robustness analysis

The robustness of cryptographic mechanisms has been analysed by DCSSI. The results are stated in the cryptographic analysis report [ANA-CRY] and lead to the following conclusion: parts of mechanisms analysed don’t reach the “standard” level as defined in DCSSI referential (see [REF-CRY]).

However, these results have been taken into account in the evaluator independent vulnerability analysis and couldn’t highlight any exploitable vulnerability for the VLA level targeted.

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality for a licensed evaluation facility. All the work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product, BULL TrustWay VPN Line, developed by Bull SAS, which may take one of following appliances form:

- TVPN appliance (Trustway Virtual Private Network) version 4.05.02,
- TCRX appliance (Trustway *Chiffreur Routeur d'eXtrémité*) version 4.05.01,
- TCRX2 appliance (2nd model of TCRX) version 4.05.01,

submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 2 augmented.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

The user of the certified product shall respect the operational environmental security objectives summarized specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- the product shall be installed, configured and maintained (application of patches or software and hardware security updates) in such a way that it preserves integrity and confidentiality of sensitive data (i.e. administration and configuration data) and of data in-transit through the product;
- administrators of the product shall be non-hostile, appropriately trained and follow all administrator guidance. In particular, authorized administrators are authenticated before performing any action on the TDM or TAM. Authentication is performed by the TDM or TAM hardware token, through a trusted path based on a smart card authentication procedure;
- all the administration equipments (TDM, CEC, TAM, SPC …) including all the associated data media (e.g. CDROM with keys, smart cards …) and the TVPN appliance shall be placed in secure environments (physical and logical measures) which access is strictly restricted to authorised administrators only. In particular, the CEC or the SPC in charge of generating the keys shall not be connected to any network. The global network security policy shall be defined appropriately, in particular, filtering equipments shall limit to the strict minimum the flows coming from a potentially hostile area to administration equipments TDM and TAM, flows udp 69 (tftp) and udp 162 (snmp) coming from fixed IP addresses, and the product shall be configured according to this policy. TDM and TAM shall provide integrity and confidentiality services in order to protect the administration dialogs with the product;

- the product shall be personalised with the SPC station in order to inject specific secrets related to one particular equipment and to one particular user. During this process, the equipment is cryptographically personalised and can be, by this way, authenticated when it will be introduced in the user network;
- the product shall use a set of keys generated by the administration station when securing communication flows with other systems. All sensitive data shall be sent encrypted as configuration elements of the product (and other systems). The renewal of keys can be realised at any time, or at a scheduled date, by updating the configuration of the product (and other systems);
- the product shall set up the appropriate configuration of Tripwire software which periodically verifies the integrity of the software which implements the product's security functions;
- cryptographic keys distributed to the product must have been generated according to recommendations specified in the DCSSI cryptographic referential (see [REF-CRY]) for the standard strength level;
- the auditors on TDM, syslog stations and supervisor stations must regularly analyse the log files. They are in charge of managing the log files and detecting any attack;
- the administrator must manage a blacklist on the TDM in order to control (accept or forbid) equipments introduction into the network;
- upon suppression of an equipment from the network (e.g. for maintenance purpose), the administrator must depersonalize this equipment before returning it to the manufacturer and must include it in the revocation list of the TDM and TAM stations.

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

IT
Security
Certified

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

[1] The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

[2] The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 2+	Intitulé du composant
ACM Configuration management	ACM_AUT				1	1	2	2		
	ACM_CAP	1	2	3	4	4	5	5	2	Configuration items
	ACM_SCP			1	2	3	3	3		
ADO Delivery and operation	ADO_DEL		1	1	2	2	2	3	1	Delivery procedures
	ADO_IGS	1	1	1	1	1	1	1	1	Installation, generation and start-up procedures
ADV Development	ADV_FSP	1	1	1	2	3	3	4	1	Informal functional specification
	ADV_HLD		1	2	2	3	4	5	2	Security enforcing high-level design
	ADV_IMP				1	2	3	3	1*	Subset of the implementation of the TSF
	ADV_INT					1	2	3		
	ADV_LLD				1	1	2	2	1*	Descriptive low-level design
	ADV_RCR	1	1	1	1	2	2	3	1	Informal correspondence demonstration
	ADV_SPM				1	3	3	3		
AGD Guidance	AGD_ADM	1	1	1	1	1	1	1	1	Administrator guidance
	AGD_USR	1	1	1	1	1	1	1	1	User guidance
ALC Life-cycle support	ALC_DVS			1	1	1	2	2	1	Identification of security measures
	ALC_FLR								3	Systematic Flow remediation
	ALC_LCD				1	2	2	3		
	ALC_TAT				1	2	3	3	1*	Well-defined development tools
ATE Tests	ATE_COV		1	2	2	2	3	3	1	Evidence coverage
	ATE_DPT			1	1	2	2	3		
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing – sample
AVA Vulnerability assessment	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	1	Examination of guidance
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	2	Independent vulnerability analysis

*applied to FCS requirements

Annex 2. Evaluated product references

[2004/30]	DCSSI certificate delivered on 21 septembre 2004 for BULL Trustway VPN Appliance v3.01.06 product
[ST]	Reference security target for the evaluation: - BULL Trustway VPN Line - Security Target, - reference D00G007, - version 2.9 of 27/02/2008 (document referenced [IN.103] in the [ETR])
[ETR]	Evaluation technical report : - Rapport Technique d'Evaluation – Projet ALTAIR2, - reference OPPIDA/CESTI/ALTAIR2/RTE/2, - version of 23/09/2008 (document referenced [OUT.037] in the [ETR])
[ANA-CRY]	Cryptographic mechanisms analysis report: - cotation de mécanismes cryptographiques ALTAIR2, - reference 1438/SGDN/DCSSI/SDS/Crypto, - version 1 of 03/07/2008 (document referenced [IN.095] in the [ETR])
[CONF]	Configuration list : - Liste de configuration des équipements TrustWay VPN, - reference D00P018, - revision 1.10 (document referenced [IN.102] in the [ETR])
[GUIDES]	Product administration and installation guide: - Manuel d'installation TrustWay VPN et TrustWay CRX ou CRX2, - reference 86 F2 23ET, - version 02 (document referenced [IN.062] in the [ETR]) - Manuel d'installation et d'utilisation TDM, - reference 86 F2 26ET, - version 03 (document referenced [IN.073] in the [ETR]) Product user guide: - TDM-TAM Journalisation, Description des enregistrements - reference 86 X2 31ET 00, - version nov. 06 (document referenced [IN.045] in the [ETR]) - Manuel de dépannage TrustWay VPN et TrustWay CRX ou CRX2, - reference 86 F2 27ET, - version 02 - (document referenced [IN.049] in the [ETR])

Annex 3. Certification references

Decree number 2002-535 dated 18th April 2002 related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. The content of Common Criteria version 2.3 is identical to the international ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. The content of CEM version 2.3 is identical to the international ISO/IEC 18045:2005.
[CC RA]	Arrangement on the Recognition of Common criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	«Mutual Recognition Agreement of Information Technology Security Evaluation Certificates», version 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level version 1.10, 14th of September 2007, No. 1904/SGDN/DCSSI/SDS/LCR