17 FEB 2011

I. GEGEVENS AANVRAAG

Nummer aanvraag : 10 2 g
Datum aanvraag : 19-01-2011
Land eindbestemming : Wereld m.u.v. moeilijke landen
Land van bestemming : Wereld m.u.v. moeilijke landen

Datum voorlegging : 16-02-2011
Regime/subregime : W 000
S.G.-postnummer : 5A002a7
Land van oorsprong : Nederland
Goederenomschrijving: Fort Fox Hardware Data Diode; FFHDD2+
Hoeveelheid : 10
Waarde + valuta : 10 1 c, 10 2 g
Exporteur : Fox Crypto BV, Delft

Ontvanger : klanten Fox Crypto

Eindgebruiker :

Eindgebruik : koppelen van hoog gerubriceerde netwerken aan laag gerubriceerde netwerken

Aard van transactie : Verkoop

Contactpers. bedrijf: 10 2 e
Telefoonnummer :

II. BESLISSING BEB/HPG

Beslissing : Toewijzen / ~~Afwijzen~~
Naam : 10 2 e
Datum : 21-2-2011
Handtekening :

Condities : 10 2 e

Voorgelegd AIVD/ECD : J[] / N[]

Getoetst door : 10 2 e
21/02/2011
10 2 e

III. PRE-ADVIES CDIU

Risk Report

Eindgebruiker	:n.v.t.
Land	:n.v.t.
Programma	:n.v.t.
Int. Regime	:n.v.t.
Onderzoek InL.Dienst	:nee
Vergunningenoverzicht	:geen
Toewijzingen	:n.v.t.
Afwijzingen NL	:n.v.t.
Advies CDIU	:akkoord
Overige informatie	:Stukken worden nagezonden. Het product is recentelijk goedgekeurd voor EAL 7+. Hierdoor is het op de lijst van Dual-use goederen gekomen. Het product is door certificering op de Cryptolijst gekomen terwijl het geen crypto bevat. Het beschermt netwerken gebaseerd op de wetten van de fysica en niet met crypto.
Denial eindgebruiker	:n.v.t.
Denial land van best.	:n.v.t.
Nummer (EU)-Denial(s)	:n.v.t.
Naam behandelaar CDIU:	102e [redacted]
Sondage	: N [x] J [] Nummer sondage:
Eventuele condities	:

INFORMATIE BIJ CRYPTO-AANVRAAG

Bijlage bij vergunningaanvraag nummer: 102g [redacted]

Technisch contactpersoon bedrijf
naam:
tel:

A. Goederenomschrijving

Naam product :
Type-en versienummer :

Lijst van bijgevoegde folders en beschrijvingen (van product, algoritme en sleutelmanagement):
1.
2.
3.

B. Voor het hierboven omschreven product is eerder vergunning verstrekt: [] J [] N onder nummer:

C. Gegevens eindgebruiker
Naam :
Doelgroep : [] financiele instelling
[] overheidsinstelling
[] bedrijf
[] particulier

D. Cryptographische gegevens

Crypt. beveiligingsfuncties(s) : [] encryptie
[] key management
[] authenticatie/integriteit
[] identificatie
[] PIN/MAC/Access
[] digitale handtekening

Primaire functie : [] communicatie
[] opslag

Implementatie : [] hardware/firmware
[] software

Naam toegepast cryptographisch algoritme(n):
Naam toegepast sleutelmanagement :
Korte beschrijving sleutelmanagement :
Symmetrische sleutellengte :
Asymmetrische sleutellengte :
Voldoet het cryptoproduct aan de voorwaarden van paragraaf a, b en c van de cryptografienoot: [] Ja [] Nee
US Licence ENC : [] Ja [] Nee

3

TNO CERTIFICATION

Laan van Westenenk 501
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

Phone +31 55 5493468
Fax +31 55 5493288
E-mail: Certification@certi.tno.nl

BTW/VAT NR NL8003.32.167.B01
Bank ING at Delft
Bank account 66.77.18.141
stating 'TNO Certification'
BIC of the ING Bank: INGBNL2A
IBAN: NL81INGB0667718141

Date
June 16, 2010

Reference
NSCIB-CC-09-11025-CR2

Project number
11025

Subject

NSCIB-CC-09-11025

Certification Report

Fort Fox Hardware Data Diode, version FFHDD2+

TNO CERTIFICATION

TNO CERTIFICATION
HEREBY DECLARES THAT EVALUATION
HAS DEMONSTRATED THAT THE PRODUCT

Fort Fox Hardware Data Diode, version FFHDD2+, Assurance Package: EAL7 augmented with ALC_FLR.3 and ASE_TSS.2
Product and version

FROM

Fox-IT BV located in Delft, the Netherlands
Sponsor's name and address

COMPLIES WITH THE

Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 2
Certification guidelines or standards

AS DEMONSTRATED BY / EVALUATION PERFORMED BY

Brightsight BV located in Delft, the Netherlands
Testing Laboratory

APPLYING THE

Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 2

NSCIB-CC-09-11025-CR2
Certification Report number

THE CERTIFICATE HAS BEEN ISSUED ON

September 7, 2009
1st Issue Date

June 16, 2010
Revision Date

September 7, 2019
Expiry Date

ISSUED IN: Apeldoorn, the Netherlands

DIRECTOR TNO CERTIFICATION

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 2 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 2. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TNO Certification or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TNO Certification or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

CERTIFICATE NUMBER CWA 15525

ACCREDITED BY THE DUTCH RAD FOR ACCREDITATION

Table of contents

Table of contents 3
Document Information 3
Foreword 4
Recognition of the certificate 4
1 Executive Summary 5
2 Certification Results 6
2.1 Identification of Target of Evaluation 6
2.2 Security Policy 6
2.3 Assumptions and Clarification of Scope 6
2.3.1 Usage assumptions 6
2.3.2 Environmental assumptions 6
2.3.3 Clarification of scope 7
2.4 Architectural Information 7
2.5 Documentation 7
2.6 IT Product Testing 8
2.6.1 Testing approach 8
2.6.2 Test Configuration 8
2.6.3 Depth 8
2.6.4 Independent Penetration Testing 8
2.6.5 Testing Results 9
2.7 Evaluated Configuration 9
2.8 Results of the Evaluation 9
2.9 Evaluator Comments/Recommendations 10
2.9.1 Obligations and hints for the developer 10
2.9.2 Recommendations and hints for the customer 10
3 Security Target 11
4 Definitions 11
5 Bibliography 11

Document Information

Date of issue	16 June 2010
Author	R.T.M. Huisman
Version of report	2
Certification ID	NSCIB-CC-09-11025
Sponsor and Developer	Fox-IT BV
Evaluation Lab	Brightsight BV
TOE name	Fort Fox Hardware Data Diode, version FFHDD2+
Report title	Certification Report
Report reference name	NSCIB-CC-09-11025-CR2

6

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TNO Certification has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations in the Netherlands are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TNO Certification in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TNO Certification to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TNO Certification asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European Recognition Agreement approved by the SOG-IS in April 1999 provides mutual recognition of ITSEC and Common Criteria certificates for all evaluation levels (E6, resp. EAL7). This agreement was originally signed by Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Fort Fox Hardware Data Diode, version FFHDD2+. The developer of the FFHDD2+ is Fox-IT BV located in Delft, the Netherlands and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The FFHDD2+ is evaluated on the assurance level EAL7+ and builds on the evaluation results of the recently performed evaluation of the Fort Fox Hardware Data Diode, version FFHDD2. This previous version was certified on September 7th 2009 on the assurance level EAL4+ under the same certification identifier NSCIB-09-11025 with an certification report identified as 'version 1'. Version FFHDD2+ of the TOE is identical to the previous version FFHDD2 except for the addition of a new front panel and the guidance documentation describing this additional front panel. The original certification report NSCIB-CC-09-11025 version 1 has now been extended to cover the Fort Fox Hardware Data Diode, version FFHDD2+ as described in this document, certification report NSCIB-CC-09-11025 version 2.

The Target of Evaluation – TOE (i.e., Fort Fox Hardware Data Diode) is a hardware-only device that allows data to travel only in one direction. The intention of is to let information be transferred optically from a low security classified network (Low Security Level) to a higher security classified network (High Security Level), without compromising the confidentiality of the information on the High Security Level. Once manufactured, there is no way to alter the function of the TOE.

The TOE has been re-evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on 10 June 2010. The evaluation builds upon the EAL4+ evaluation that was completed on 21 August 2009 as described in version 1 of this Certification Report. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The certification was completed on 16 June 2010 with the preparation of version 2 of this Certification Report.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Fort Fox Hardware Data Diode, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Fort Fox Hardware Data Diode are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets the Evaluation Assurance Level (EAL) 7 assurance requirements augmented with ALC_FLR.3 and ASE_TSS.2 for the evaluated security functionality. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 2 *[CC]*.

TNO Certification, as the NSCIB Certification Body, declares that the Fort Fox Hardware Data Diode version FFHDD2+ evaluation meets all the conditions for international recognition of Common Criteria certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 7 augmented with ALC_FLR.3 and ASE_TSS.2 evaluation is the Fort Fox Hardware Data Diode, version FFHDD2+ from Fox-IT BV located in Delft, the Netherlands.

This report pertains to the TOE comprised of the following main component:

Item	Identifier	Version	Medium
Hardware	Fort Fox Hardware Data Diode	FFHDD2+	single 19-inch rack component

To ensure secure usage a guidance document is provided together with the Fort Fox Hardware Data Diode. Details can be found in section 2.5 of this report.

2.2 Security Policy

The TOE is the Fort Fox Hardware Data Diode (FFHDD) and allows data to travel only in one direction. The intention of is to let information be transferred optically from a low security classified network (Low Security Level) to a higher security classified network (High Security Level), without compromising the confidentiality of the information on the High Security Level. Once manufactured, there is no way to alter the function of the TOE.

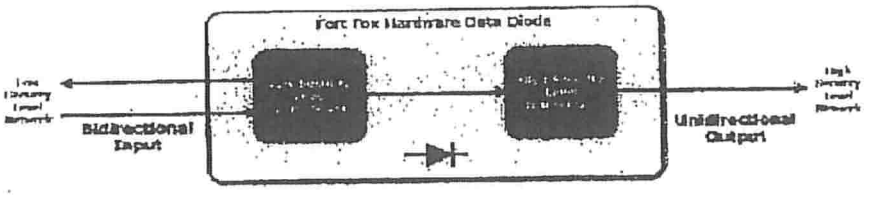


Figure 1, Overview of the TOE.

2.3 Assumptions and Clarification of Scope

2.3.1 Usage assumptions

There are no usage assumptions identified in the Security Target that are of relevance to the TOE.

2.3.2 Environmental assumptions

The following assumptions about the environmental aspects defined by the Security Target have to be met (for the detailed and precise definition of the assumptions refer to the *[ST]*, chapter 3.3):

> The intended operation environment shall store and operate the TOE in accordance with the requirements of the High Security Level side.
>
> The TOE is the only method of interconnecting the Low Security Level network and High Security Level network. This prevents a threat agent from circumventing the security being provided by the TOE through an untrustworthy product.

2.3.3 Clarification of scope

There are no defined threats for the TOE that require additional measures in the environment, they are all met by the TOE. The Security Target [ST] assumes an operational environment such that threats could come only from the attached networks. The evaluation did not reveal any functionality in the TOE that was excluded from the TOE evaluated configuration.

2.4 Architectural Information

The TOE is a single 19" rack component, a hardware-only device. To ensure signals can only pass in one direction, but not vice versa, the TOE deploys a light source and corresponding photocell. The data transfer is implemented in hardware, of the physical Open System Interconnection (OSI) reference model, to guarantee complete unidirectionality. Fiber-optic cables are used to minimize the electromagnetic radiation when the TOE input is connected to the Low Security Level Server and the TOE output is connected to the High Security Level Server.

The TOE has two operational interfaces to establish one-way communication, the Bidirectional Input and Unidirectional Output port. At the Low Security Level Transceiver light is carried into the Bidirectional Input port and converted, with the aid of a photocell, into an electrical signal. The electrical signal spreads through the TOE to the High Security Level Transceiver. The High Security Level Transceiver receives the electrical signal and converts this, using a light source, into light. Finally, the light is offered, through the Unidirectional Output port, to the High Security Level Network.

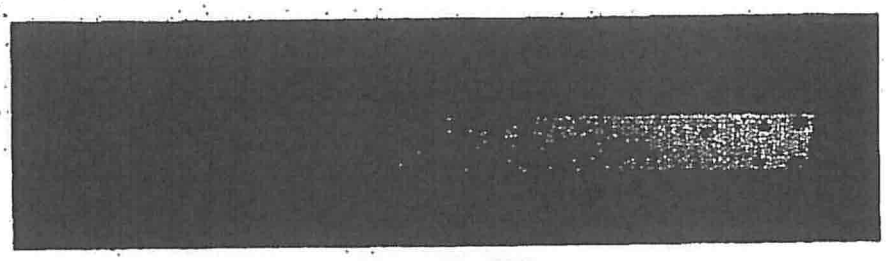


Figure 2 The TOE

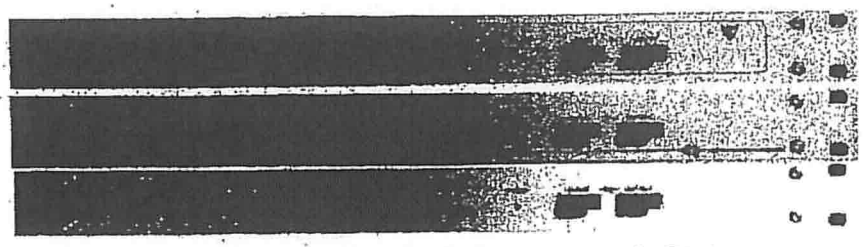


Figure 3 Three variants for the front panels of the TOE

2.5 Documentation

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

Identifier	Version
Fox-IT BV, FFHDD, Delivery Procedures, Preparative Procedures and Operational User Guidance, CC EAL7+	2.02, June 3, 2010

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach

The evaluator has tested all interfaces of the TOE and tested all six tests defined by the developer. In addition four tests are defined to extend the rigor of testing done by the developer.

Before these tests were conducted it was verified that the TOE was suitable for testing and has a unique reference number as identified in the ST introduction.

2.6.2 Test Configuration

The test configuration for the independent testing comprised of two configurations. The non-TOE servers for the High Security Level side and Low Security Level side were included in both test setups.

Test configuration 1 was the configuration as delivered to a customer and was used for testing the external interfaces for all TSFI.

Test configuration 2 was using an additional Fort Fox Hardware Data Diode of which the output side was connected to the output of the TOE. This setup was used to test the interfaces of the SFR-enforcing module.

2.6.3 Depth

For this evaluation, the depth of testing relates to the TSF modules and the SFR-enforcing module in the TOE design. The TOE Design defines two simple sets of modules for the TOE. The first set concerns the power supply; the second concerns the data diode.

All modules are SFR-supporting, except for one security-enforcing module in the data diode set of modules and this module has been tested.

In one of the tests it is checked that all the components in the design documentation are indeed implemented in FFHDD2+. In this test the implementation representation is tested exhaustively.

2.6.4 Independent Penetration Testing

The evaluators considered the following possible attacks:

1. Attack from the low security level network trying to compromise the TOE such that it passes information through from the high security level network;
2. Attack from the high security level network trying to compromise the TOE such that it passes information through from the high security level network;
3. Attack from bystanders by the TOE to eavesdrop information passing through the TOE;
4. Trying to cause TOE failure such that the TOE comes in a state that it passes information through from the high security level to the low security level.

The TOE design shows that one electronic component is essential in the realisation of ensuring that signals can only pass in one direction, and not vice versa. The evaluators have chosen to test the resistance of the TOE against the introduction of light signals at the Output port. If these signals would pass through the TOE, they could influence the signals as emitted by the bi-directional Input. This

attack relates to the possible attacks 1, 3 and 4 listed above. Attack 2 is out of scope due to the objectives of the environment.

2.6.5 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests. No residual vulnerabilities were found.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Fort Fox Hardware Data Diode, version FFHDD2+ and can be identified by its identification at the backside.

The TOE needs no specific configuration settings because there is only one configuration defined.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references several Intermediate Reports. The verdict of each claimed assurance requirement is given in the following table:

[illegible]		[illegible]
Development		**Pass**
Security architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.6	Pass
Implementation representation	ADV_IMP.2	Pass
Internals	ADV_INT.3	Pass
Security Policy Model	ADV_SPM.1	Pass
TOE design	ADV_TDS.6	Pass
[illegible]		[illegible]
Operational	AGD_OPE.1	Pass
Preparative	AGD_PRE.1	Pass
[illegible]		[illegible]
Configuration Management Capabilities	ALC_CMC.5	Pass
Configuration Management Scope	ALC_CMS.5	Pass
Delivery	ALC_DEL.1	Pass
Development Security	ALC_DVS.2	Pass
Flaw remediation	ALC_FLR.3	Pass

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Lifecycle definition	ALC_DEL.2	Pass
Tools and Techniques	ALC_TAT.3	Pass

Coverage	ATE_COV.3	Pass
Depth	ATE_DPT.4	Pass
Functional	ATE_FUN.2	Pass
Independent	ATE_IND.3	Pass

Vulnerability analysis	AVA_VAN.5	Pass

Based on the above evaluation results the evaluation lab concluded the Fort Fox Hardware Data Diode, version FFHDD2+, to be **CC Part 2 conformant, CC Part 3 conformant,** and to meet the requirements of **EAL 7 augmented with ALC_FLR.3 and ASE_TSS.2**. This implies that the product satisfies the security technical requirements specified in Security Target FFHDD, CC EAL7+, version 2.04, June 3, 2010. The Security Target does not claim conformance to any Protection Profile.

2.9 Evaluator Comments/Recommendations

2.9.1 Obligations and hints for the developer

Based on the insights gained during the evaluation the evaluator recommends for the protection of configuration items at Fox-IT to extend the current anti-virus measures in a similar way to non-Windows platforms.

2.9.2 Recommendations and hints for the customer

The TOE is normally delivered together with the two servers. These servers are connected to the network that the TOE connects. These servers are not considered during the evaluation.

3 Security Target

The Security Target FFHDD, CC EAL7+, version 2.04, June 3, 2010 is included here by reference. Please note that for the need of publication a public version has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

CC	Common Criteria
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
PP	Protection Profile
TNO	Netherlands Organization for Applied Scientific Research
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Part I version 3.1 revision 1, and Parts II and III, version 3.1 revision 2.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 2, September 2007
[ETR]	Evaluation Technical Report, Fort Fox Hardware Data Diode FFHDD2+ - EAL7+, Version 2.0, June 10, 2010.
[NSCIB]	Nederlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004.
[ST]	Fox-IT BV, FFHDD, Security Target, CC EAL7+, version 2.04, June 3, 2010.
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

FOX-IT
EXPERTS IN IT SECURITY

PRO FORMA INVOICE

101 c, 102 g

[redacted]

I voic

Fox Crypto B.V.
Olof Palmestraat 6, 2616 LM
P.O. box 638, 2600 AP Delft
The Netherlands

Tel.: +31 (0)15 284 79 99
Fax: +31 (0)15 284 79 90
Email: crypto@fox-crypto.com
Web: www.fox-crypto.com

ABN-AMRO
no. 61.01.62.179
Chamber of Commerce
Hanglanden no. 27162642

5A002 a. 1. *(vervolg)*

3. *Tot "cryptografie" worden niet gerekend: technieken van "vaste" gegevenscomprimering of -codering.*

Noot: 5A002.a.1. is ook van toepassing op apparatuur die is ontworpen of aangepast voor het gebruik van "cryptografie" op grond van analoge principes, wanneer deze met behulp van digitale technieken worden toegepast.

a. Een "symmetrisch algoritme" met een sleutellengte van meer dan 56 bits; of

b. Een "asymmetrisch algoritme" waarvan de beveiliging wordt gewaarborgd door:

1. Ontbinding van gehele getallen van meer dan 512 bits (bv. RSA)

2. Berekening van discrete logaritmen in een groep van een eindig veld met een grootte van meer dan 512 bits (bv. Diffie-Hellman over Z/pZ); of

3. Discrete logaritmen in een andere dan de in 5A002.a.1.b.2 genoemde groepen van meer dan 112 bits (bv. Diffie-Hellman over een elliptische curve);

2. ontworpen of aangepast voor het uitvoeren van cryptanalytische functies;

3. niet gebruikt;

4. speciaal ontworpen of aangepast voor het reduceren van ongewenste lekken van informatiedragende signalen, afgezien van hetgeen noodzakelijk is om aan de normen voor gezondheid, veiligheid en elektromagnetische interferentie te voldoen;

5. ontworpen of aangepast voor het hanteren van cryptografische technieken voor het genereren van de spreidcode voor "spread spectrum"-systemen, met uitzondering van de technieken vermeld in 5A002.a.6., met inbegrip van de hopping-code voor "frequency hopping"-systemen;

6. ontworpen of aangepast voor het gebruik van cryptografische technieken om kanaliseringscodes versleutelingscodes of netwerkidentificatiecodes te genereren voor systemen die gebruik maken van ultrabreedband-modulatietechnieken, met een van de volgende kenmerken:

a. een bandbreedte van meer dan 500 MHz; of

b. een "fractionele bandbreedte" van 20 % of meer;

7. niet-cryptografische beveiligingssystemen en -voorzieningen voor informatie- en communicatietechnologie (ICT), met een beveiligingsniveau hoger dan of gelijkwaardig aan klasse EAL-6 (evaluation assurance level) van de Common Criteria;

8. communicatiekabelsystemen die met mechanische, elektrische of elektronische middelen zijn ontworpen of aangepast, voor het opsporen van clandestiene binnendringing;

9. ontworpen of aangepast om "kwantumcryptografie" te gebruiken.

Technische noot:

"Kwantumcryptografie" wordt ook aangeduid als <quantum key distribution (QKD)>.

Noot: In 5A002 zijn niet bedoeld:

a. "persoonsgebonden slimme kaarten" met een van de onderstaande kenmerken:

1. waarvan de cryptografische functie beperkt is tot het gebruik in apparatuur of systemen die van embargo zijn uitgesloten krachtens de punten b. tot en met g. van deze noot; of

(3)

16

10 2 e [redacted]

Van: namens Vergunningen
Aan: 10 2 e [redacted].@BELASTINGDIENST.NL
Onderwerp: RE: 2875-9509 W Wereld

t.a.v. 10 2 e [redacted]

II. BESLISSING BEB/HPG

Beslissing : Toewijzen
Naam : 10 2 e [redacted]
Datum : 21-02-2011

(4)

17

24 APR 2012

I. GEGEVENS AANVRAAG

Nummer aanvraag	: 10 2 g [redacted]
Datum aanvraag	: 28-03-2012
Land eindbestemming	: wereld muv de bad-guy landen
Land van bestemming	: wereld muv de bad-guy landen
Datum voorlegging	: 24-04-2012
Regime/subregime	: W 000
S.G.-postnummer	: 5A002a7
Land van oorsprong	: Niet Nader Bepaalde Landen
Goederenomschrijving	: Apparatuur voor informatie beveiliging
Hoeveelheid	: 10 1 c [redacted]
Waarde + valuta	:
Exporteur	: Fox Crypto BV Delft
Ontvanger	: klanten van fox Crypto
Eindgebruiker	: idem
Eindgebruik	: informatie-beveiliging
Aard van transactie	: verkoop
Contactpers. bedrijf	: 10 2 e [redacted]
Telefoonnummer	:

10 1 c, 10 2 g [redacted]

19/6 Met 10 2 e [redacted] gebeld voor 6barbus. Voicemail ingesproken.

II. BESLISSING IB/IMH

Beslissing	: ~~Toewijzen / Afwijzen~~ Vervallen
Naam	: 10 2 e [redacted]
Datum	: 19-07-2012
Handtekening	: 10 2 e [redacted]
Condities	: Bedrijf dient aangepaste aanvraag in. Opbezoek geweest bij EL&I d.d. 13/4
Voorgelegd AIVD/POSS	: J[] / N[]
Collegiale toets	:

27/6 Bedrijf gaat nieuwe aanvraag indienen; 10 2 e [redacted] stelt voor geen algemene vergunning af te geven, omdat hij wil weten wie wat ontvangt.

* Zijn er afspraken gemaakt tussen 10 1 c, [redacted] en bedrijf?
* Om hoeveel aanvragen gaat het per jaar?
=> Daarom bedrijf bellen.
* Dit bedrijf heeft geen contractuele verplichtingen

29/6 Gesprek 10 2 e [redacted]

EAL
1 Datadiode, hoogwaardige technologie, level 7, behoort tot top 3 in de wereld
2 Redfox hoogwaardige crypto, stg nieuw, gemaakt in opdracht 10 1 [redacted]
3 Skytale hoogwaardige crypto, voor lage bandbreedte en instabiel signaal hoog wel kwa, ook in opdracht 10 1 [redacted]

2.0.2.

5

18

17/7

Gesprek [redacted]

~ [redacted]

~ Betreft Datadiode en Redfox

Datadiode: Hoge certificering, [redacted]

Redfox: universeel blokje dat crypto regelt

6

III. PRE-ADVIES CDIU

Risk Report : nvt
Eindgebruiker :

Land : Diverse Landen
Programma :
Int. Regime :
Onderzoek InL.Dienst :

Vergunningenoverzicht:
Toewijzingen : 2875 9509 dd 19-01-2011
Afwijzingen NL : geen
Advies CDIU : toewijzen

Overige informatie : crypto-fml. volgt per fax
Denial eindgebruiker : nvt
Denial land van best.: nvt
Nummer (EU)-Denial(s): toewijzen

Naam behandelaar CDIU: 102e [redacted]

Sondage : N [X] J [] Nummer sondage:

Eventuele condities :

INFORMATIE BIJ CRYPTO-AANVRAAG

Bijlage bij vergunningaanvraag nummer: [redacted]

Technisch contactpersoon bedrijf
naam: [redacted]
tel:

A. Goederenomschrijving
Naam product :zie fax
Type-en versienummer :zie fax

Lijst van bijgevoegde folders en beschrijvingen (van product, algoritme en sleutelmanagement):
1.
2.
3.

B. Voor het hierboven omschreven product is eerder vergunning verstrekt: [X] J [] N onder nummer:
2875 9509

C. Gegevens eindgebruiker
Naam :
Doelgroep :
[X] overheidsinstelling
[X] niet overheidsinstelling

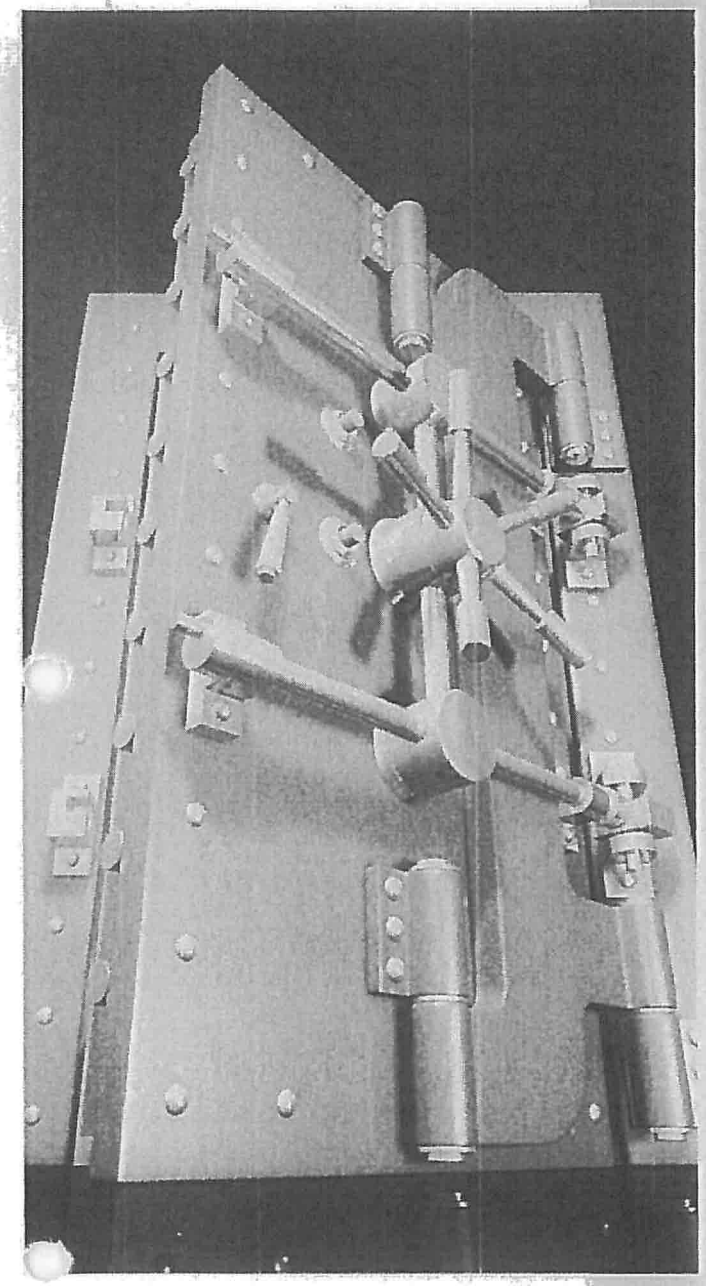
D. Cryptographische gegevens

Crypt. beveiligingsfuncties(s) :
[] encryptie
[] key management
[] authenticatie/integriteit
[] identificatie
[] PIN/MAC/Access
[] digitale handtekening

Primaire functie :
[] communicatie
[] opslag

Implementatie :
[] hardware/firmware
[] software

Naam toegepast cryptographisch algoritme(n): nvt er zit geen algoritme in
Naam toegepast sleutelmanagement : nvt
Korte beschrijving sleutelmanagement :
Symmetrische sleutellengte :
Asymmetrische sleutellengte :
US Licence ENC : [] Ja [X] Nee
Welk deel van paragraaf 740.17 EAR : [] a1 [] a2
: [] b1 [] b2i [] b2ii [] b2iii
: [] b2ivA [] b2ivB [] b3 [] b4



The next-generation cryptographic platform for high-security products

RedFox Cryptographic Platform

Creating certified cryptographic products used to be a complex task, especially if you require a certification for government use. Not only must the products provide unsurpassed levels of security, but they must also undergo lengthy evaluations by various certification bodies. This often leads to a very long time to market. A lot of time, and thus money, is spent before the end-user benefits from your cryptographic solution.

Fox-IT has developed the RedFox carrier module in close cooperation with the Dutch government. The RedFox allows for swift certification of products based on it. The RedFox offers very high levels of security, both logical and physical. Cryptographic algorithms are implemented in hardware and provide high-performance throughput up to 800 Mbit/sec. Integrating the RedFox into new high-security products is a straightforward task using the SDK and reference implementations, thereby allowing time to market to be reduced significantly.

FOX-IT
FOR A MORE SECURE SOCIETY

(7)

Many security products require strong cryptography. Providers of such products and their customers need to rely on a strong cryptographic core. This ensures that their products are truly secure. Examples of such high security products abound, both in government and commercial settings. These include VPN solutions, hard disk encryption and hardware security modules (HSMs).

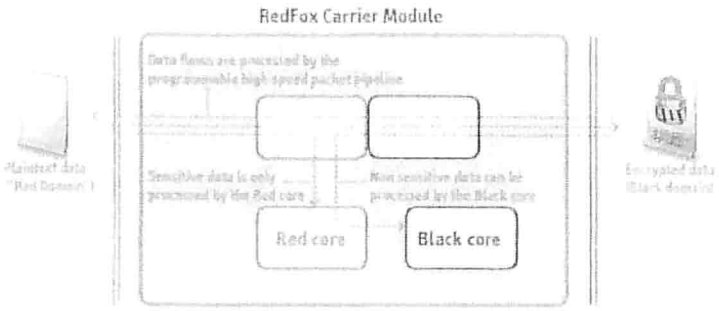
As cryptography lies at the heart of these products, government or commercial evaluations of such products focus heavily on the strength of the underlying cryptographic system. There are good reasons for this focus. Although modern cryptographic algorithms are theoretically strong, many mistakes can be made in their implementation.

A common solution to this problem is to offload cryptographic operations to a trusted external hardware security module (HSM). However, traditional HSMs cannot implement complex data processing logic, do not provide strict red-black separation, and do not offer flexible hardware interfacing. They must therefore be integrated into a host system that provides these features, thereby extending the scope of the security functionality to include the HSM and host system. That complicates the security design, makes it more difficult to ensure correct implementation, and increases the cost of certification and the time to market.

The RedFox Carrier Module (RF-CM) is a flexible HSM designed to be used as a building block in a wide variety of products. It can run complex data processing logic and provides strict red-black separation in hardware. The RF-CM was developed in close cooperation with the Dutch National Communications Security Agency (NL-NCSA). As such, it is designed to be used at the highest levels of Dutch, EU, and NATO security. The RF-CM is available in two editions to suit both government and enterprise customers.

Architecture

The RF-CM contains two separate processor cores to ensure very strong red-black separation (see figure). The red core handles sensitive data, such as keys or unencrypted data, while the black core processes non-sensitive data. This ensures that even if the black core is compromised, both key material and sensitive data remain secure.



Aside from the red and black cores, a programmable packet processing pipeline allows high-speed cryptographic operations. This pipeline, known as the hardware fast-path, can be programmed to process and encrypt data packets at high speed (up to 800 Mbit/second). Each packet is initially matched and assigned to a certain flow. Known flows can then be automatically decrypted or encrypted in hardware, without the need to query the red or black cores. Flows that require further processing can be offloaded to the red or black core, depending on the sensitivity of the data. As this process is highly flexible, the hardware fast-path can be used for a wide range of applications, including network-based products, hard disk encryption, key management and more.

Shortening time to market for certified security products

Due to its flexible nature, the RF-CM can be used as a solid base for security products requiring cryptography or secure storage. It is well-suited for NATO, EU and NL national markets.

The RF-CM has been developed in close cooperation with the NL-NCSA. This ensures that the certification of end-products based on the RF-CM can be performed much more cost-effectively than a fully custom solution. The RF-CM comes with approved pre-certification documentation, ensuring that the most complex parts of end-product certification can be performed rapidly.

Challenges in high-security products

Creating high-security products is a challenging task. A single flaw in either design or implementation can have catastrophic consequences for the system's security. Especially challenging aspects include the secure implementation of cryptographic logic, multiple layers of strong physical defenses, and perhaps most of all the protection of sensitive (red) data and processing logic and separation thereof from the non-sensitive, untrusted (black) domain.

The modern computing platform generally provides a single processor on which software runs, and it is the software's responsibility to provide data protection. This design has significant weaknesses and, as the software becomes more complex, can make certification very difficult. Software bugs can lead to breaches of security and data loss because the hardware doesn't enforce security domain separation. Unexpected hardware behavior can make well-written software vulnerable to specialist attacks, such as cache timing or other side-channel attacks.

Even many existing high-security products contain only a single processor and cannot run red and black software separately. That leads to highly critical security logic and more complex noncritical support logic being mixed, thereby complicating the certification process and increasing the chance of undetected flaws.

FOX-IT
FOR A MORE SECURE SOCIETY

The RF-CM provides a complete package containing thoroughly evaluated high-performance cryptographic hardware and distinct red and black processing cores for running application-specific software in both domains without breaking the strict hardware-enforced domain boundary. All of this is wrapped in multiple layers of strong physical protection.

Unsurpassed levels of security

The RF-CM contains a large number of security and anti-tamper measures at the physical, electrical, and software levels (see highlight: Security in Depth). The security is active and, on detection of an attempt to tamper with the device, all sensitive material within the device is immediately cleared.

To ensure that the software on the system can be trusted, every step of the software chain can only run if it has a correct digital signature. The system is a trusted platform, ensuring that malicious code cannot be executed. Further security measures include support for a Crypto Ignition Key (CIK) which is stored on a hardware device that, when removed, renders the device unclassified. Keeping the CIK and the RF-CM separate ensures additional security during transport and storage.

Security in Depth

Strong security consists of multiple layers, ensuring that even if several countermeasures fail, an attacker cannot access the sensitive material contained in the device. The RF-CM contains many state-of-the-art security measures at the physical, electrical and logical levels.

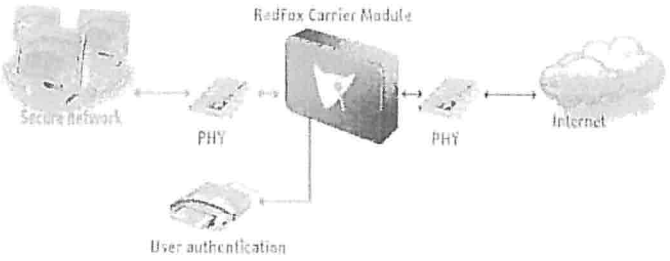
Red-Black separation

The RF-CM's security philosophy is based on a clear boundary between a sensitive (red) domain and a non-sensitive (black) domain. The red domain handles sensitive information such as key material, authentication and unencrypted data. The black domain only handles non-sensitive information, such as encrypted data. The boundary between the red and black domains is enforced in hardware, with crossings strictly controlled and kept to a minimum.

Example: VPN solution

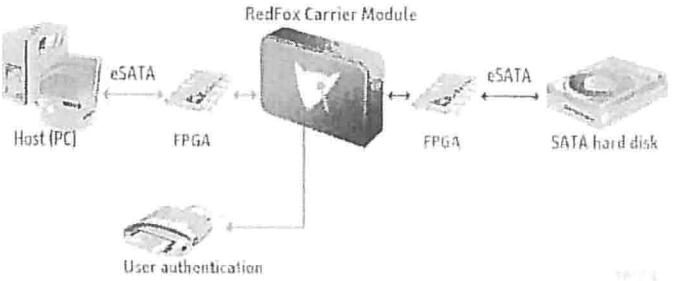
The red and black Gigabit Ethernet interfaces and the design of the hardware fast-path make the RF-CM a perfect fit for network encryption. A high-security Virtual Private Network (VPN) requires minimal extra hardware besides the RF-CM due to the built-in red and black processor cores. Only an interface for user authentication and the physical Ethernet drivers for fiber or copper media are required to complete the hardware design for a VPN appliance.

The VPN endpoint software that runs on the RF-CM's red and black cores can be cost-effectively built on top of the !RedFox SDK, thereby minimizing software development effort necessary for creating a fully functional VPN solution. The system's flexibility allows software to be written for both local management using a simple user interface and remote management over the wire from a management station.



Example: Hard disk encryption

The flexible design of the RF-CM also allows other uses than high-speed network encryption. One particular example is the use of the RF-CM for hard disk encryption.



The diagram above illustrates the concept of a transparent eSATA hard disk encryption device that is 'seen' by the host as a normal hard disk. The RF-CM is placed in the SATA data path. Surrounding FPGAs encapsulate eSATA frames in Ethernet frames, and vice versa. Two separate FPGAs are used to guarantee the red-black separation. The hardware fast-path is programmed to encrypt or decrypt the eSATA frames inside the Ethernet frame's payload at high speed.

FOX-IT
FOR A MORE SECURE SOCIETY

Technical Overview

Technical facts

Dimensions	144.5 x 109.0 x 22.5 mm (lxwxh)
Weight	0.4 kg
Power supply voltage	5 V
Power consumption	3 W (typical), 7.5 W (max)
Interfaces red	Gigabit Ethernet (GMII/MII), UART, GPIO
Interfaces black	Gigabit Ethernet (GMII/MII, UART, GPIO, USB, I2C, SPI

Performance

Crypto performance	800 Mbit / sec (AES + SHA, all key sizes)

Crypto algorithm support

RF-CM Edition:	Government	Commercial
AES (128, 192, 256 bit)	Yes	Yes
Classified algorithms	Yes	No
Camellia (128, 192, 256 bit)	No	Yes
SHA (224, 256, 384, 512 bit)	Yes	Yes
Public key operations, including RSA and ECC	Yes	Yes

Further information

Please contact Fox-IT if you would like a more detailed data sheet, a demonstration, proof of concept or integration details and SDK information.

FOX-IT
FOR A MORE SECURE SOCIETY

RedFox Carrier Module

- Offers unsurpassed levels of security, both logical and physical.
- Flexible and versatile cryptographic module.
- Shortens time to market for certified security products.
- Can be easily integrated into security products using development kit.

Fox-IT

Fox-IT specializes in cyber defense, IT Security, lawful interception and digital forensics solutions, providing completely secure, easy-to-use and automated products for data transport, interpretation and archiving to dozens of government defense and intelligence agencies, systems integrators and commercial organizations worldwide. Fox-IT solutions maintain the security of government systems up to "state secret level" sensitivity, critical infrastructure and process control networks and other highly confidential data. The company also provides services including IT security audits, digital forensic investigations, training programs and managed security services. Established in 1999, Fox-IT is based in the Netherlands and works with trusted partners in more than 20 countries.

Fox-IT
Olof Palmestraat 6
2616 LM Delft
The Netherlands

P.O Box 638
2600 AP Delft

t +31 (0)15 284 79 99
f +31 (0)15 284 79 90
e fox@fox-it.com

www.fox-it.com

Douane
Belastingdienst

Aanvraag
Vergunning uitvoer of doorvoer strategische goederen of sanctiegoederen

[redacted]

Gebruiksaanwijzing

Met dit formulier vraagt u aan: een uitvoer- of doorvoervergunning voor strategische goederen, goederen die vallen onder een sanctieregeling of goederen zoals beschreven in bijlage III van de verordening (EG) nr. 1236/2005. U kunt met dit formulier ook een sondage (proefaanvraag) indienen voor deze goederen.
Strategische goederen zijn:
- militaire goederen, zoals wapens, wapensystemen, technologie en software of materiaal dat specifiek voor militaire doeleinden is gemaakt (beschreven in de Gemeenschappelijke EU-lijst van Militaire Goederen);
- goederen die zowel een militaire als een civiele toepassing kunnen hebben, ook wel goederen voor tweeërlei gebruik of dual-usegoederen genoemd (beschreven in Verordening (EG) nr. 428/2009).

Dit formulier is ook voor het aanvragen van een uitvoervergunning voor programmatuur (software), technologie of technische bijstand die verband houden met strategische goederen. Een vergunning is nodig voor zowel fysieke als niet-fysieke (elektronische) overdracht van die programmatuur, technologie en technische bijstand.

Voor de uitvoer van strategische goederen kunt u twee soorten vergunningen aanvragen:
- een individuele uitvoervergunning voor een specifiek goed en een specifieke bestemming, of
- een globale uitvoervergunning voor een type of categorie goederen, voor meerdere transacties en voor uitvoer naar één of meer bestemmingen. Voor militaire goederen geldt deze vergunning alleen voor uitvoer naar NAVO-landen, Australië, Finland, Ierland, Nieuw-Zeeland, Zweden en Zwitserland.

Voorziet een bepaalde sanctieregeling in een ontheffing? Dan kunt u dit formulier ook gebruiken om de ontheffing op deze sanctieregeling aan te vragen.

Folterwerktuigen zijn goederen die gebruikt kunnen worden voor het uitvoeren van de doodstraf, voor foltering of voor andere wrede, onmenselijke of onterende behandeling. Deze goederen mogen alleen bij hoge uitzondering worden uitgevoerd. In bijlage III van verordening (EG) 1236/2005 staan goederen waarvoor u een uitvoervergunning kunt aanvragen. Voor de uitvoer van deze goederen kunt u alleen een individuele vergunning aanvragen voor een specifiek goed en een specifieke bestemming. Ook de technische bijstand die wordt verleend bij deze soort goederen valt onder de verordening.

RSIN/fiscaal nummer
Het Rechtspersonen en Samenwerkingsverbanden Informatienummer (RSIN) vervangt het fiscaal nummer. Het RSIN bestaat uit dezelfde cijfers als het fiscaal nummer. U gebruikt het RSIN bij uw contacten met de Nederlandse overheid.

Ondertekenen en indienen
U kunt dit formulier digitaal indienen via de postbus op www.antwoordvoorbedrijven.nl. U hoeft het formulier dan niet te ondertekenen.

U moet wél ondertekenen als u het ingevulde formulier print en opstuurt. Het postadres van de CDIU is:
Belastingdienst/Douane/Groningen/
team Centrale Dienst voor In- en Uitvoer
Postbus 30003, 9700 RD, Groningen

Telefoon: (088) 15 12122
Fax: (088) 15 13182

Bijlagen
Vraagt u een vergunning of ontheffing aan? Stuur dan mee met deze aanvraag:
- Een kopie van het getekende contract of de order. Is er nog geen getekend contract? Dan kunt u in afwachting hiervan een conceptcontract meesturen.
- Een verklaring over het eindgebruik van de goederen (een eindgebruikersverklaring). De verklaring moet worden gelegaliseerd door de autoriteiten of een instantie die is gemachtigd door die autoriteiten. In veel landen is dit de Kamer van Koophandel. Is de afnemer een overheidsinstantie en blijkt het eindgebruik uit het contract waarbij deze instantie partij is? Dan hoeft u een aparte eindgebruikersverklaring in veel gevallen niet mee te sturen.

Gaat de vergunningaanvraag over militaire goederen? Stuur dan ook mee:
- Een uitvoervergunning uit het land van herkomst, als deze aanwezig is.

Vraagt u geen vergunning aan maar een sondage? Dan zijn de bijlagen optioneel.

Hebt u bij een vraag niet voldoende invulruimte? Ga dan verder op een bijlage. Zet op elke bijlage uw naam en handtekening.

Gegevens aanvraag

1 Soort aanvraag

1a	Vraagt u een vergunning aan of een sondage (proefaanvraag)? *Kruis aan wat van toepassing is*	☒ vergunningaanvraag ☐ sondage (proefaanvraag)
1b	Gaat uw (proef)aanvraag over goederen of over technologie/technische bijstand? *Kruis aan wat van toepassing is, meer antwoorden zijn mogelijk*	☒ goederen ☐ technologie/technische bijstand
1c	Gaat uw (proef)aanvraag over technologie/technische bijstand? Geef dan aan hoe de overdracht van de technologie/technische bijstand plaatsvindt. *Kruis aan wat van toepassing is, meer antwoorden zijn mogelijk*	☐ fysieke overdracht ☐ niet-fysieke overdracht

2 Gegevens aanvrager (exporteur)

2a	Naam of bedrijfsnaam	FOX CRYPTO B.V.
	Adres	OLOF PALMESTRAAT 6
	Postcode en woonplaats	2616 LM DELFT
	Telefoonnummer	[redacted]
	E-mailadres	
2b	Relatiecode CDIU	[redacted]
2c	EORI-nummer of RSIN/fiscaal nummer	N[redacted]

Aanvraag Vergunning uitvoer of doorvoer strategische goederen of sanctiegoederen

3 Gegevens agent/vertegenwoordiger

3a Naam of bedrijfsnaam

Adres

Postcode en woonplaats

Telefoonnummer

E-mailadres

3b Relatiecode CDIU

3c EORI-nummer of RSIN/fiscaal nummer

4 Gegevens geadresseerde/ontvanger

Naam of bedrijfsnaam

Adres

Postcode en woonplaats

Land

5 Gegevens eindgebruiker (als deze een andere is dan de geadresseerde)

Naam of bedrijfsnaam

Adres

Postcode en woonplaats

Land

6 Individuele of globale vergunning

6a Vraagt u een individuele of een globale vergunning aan?
Kruis aan wat van toepassing is

☐ Individueel
☒ globaal

6b Uiterste maand van uitvoer: DOORLOPEND

7 Goederen

7a Omschrijving goederen: APPARATUUR VOOR INFORMATIE BEVEILIGING

Naam product: FOX DATADIODE / SKYTALE / REDFOX

Type- en verslenummer

7b Hebt u voor hetzelfde product eerder een vergunning aangevraagd?
Kruis aan wat van toepassing is

☐ Nee, *ga verder met vraag 7c*
☒ Ja

Is deze aanvraag toegewezen?

☐ Nee
☒ Ja, vergunningnummer [redacted]

7c Omschrijving van de goederen voor publicatie op de website van de overheid: APPARATUUR VOOR INFORMATIE BEVEILIGING

7d GN-code [redacted]

CAS-nummer

SG-post: 5A002.a.7

Waarde van de goederen [redacted]

Hoeveelheid

Eenheid (van de hoeveelheid)

8 Eindgebruik

Omschrijving van het eindgebruik van de goederen. *Wees hierbij zo specifiek mogelijk*: BEVEILIGDE KOPPELING VAN VERTROUWDE EN NIET-VERTROUWDE IT-OMGEVINGEN.

Omschrijving van het eindgebruik van de goederen voor publicatie op de website van de overheid: IDEM

9 Transactie

9a Land van herkomst *(indien van toepassing)*: NEDERLAND

Lidstaat waar de goederen zich bevinden: NEDERLAND

Land van bestemming: GLOBAL

Land van eindbestemming: GLOBAL

9b Soort transactie
Kruis aan wat van toepassing is. U kunt maar één optie aankruisen

- ☐ wederuitvoer/doorvoer
- ☒ definitieve uitvoer of verzending
- ☐ definitieve uitvoer of verzending voor onderhoud of reparatie
- ☐ definitieve uitvoer of verzending voor vervanging van goederen waarvoor al een uitvoervergunning is afgegeven
- ☐ tijdelijke uitvoer in het kader van een andere douaneregeling passieve veredeling dan bedoeld met code 25
- ☐ tijdelijke uitvoer in het kader van een andere douaneregeling passieve veredeling dan bedoeld met de codes 21 en 25
- ☐ uitvoer of verzending van goederen die bestemd zijn om opnieuw te worden ingevoerd in ongewijzigde staat en met volledige vrijstelling van belasting
- ☐ uitvoer of verzending van goederen die in een andere lidstaat zijn geplaatst onder de regeling passieve veredeling

9c Contractdatum: N.V.T.

9d Aanvullende informatie

10 Afgiftevorm vergunning

Afgiftevorm vergunning
Kruis aan wat van toepassing is. U kunt maar één optie aankruisen

- ☒ papier
- ☐ elektronisch *(alleen mogelijk bij uitvoeraangifte in Nederland)*

11 Ondertekening

Naam: [redacted]

Functie: PRODUCT MANAGER

Plaats en datum: DELFT 28-03-2012

Handtekening: [redacted]

Aantal bijlagen: 2 stuks

Aantekeningen (ruimte bestemd voor CDIU)

Toelichting

1 Soort aanvraag

1a Vergunningaanvraag of sondage (proefaanvraag)
Geef aan of u een vergunning aanvraagt of een sondage (proefaanvraag) voor vergunningplichtige goederen, technologie of technische bijstand.

1b Goederen of technologie/technische bijstand
Geef aan of uw (proef)aanvraag over goederen gaat of over technologie/technische bijstand.

1c Overdracht technologie/technische bijstand
Geef aan op welke manier de technologie/technische bijstand wordt overgedragen. Fysieke overdracht gaat met een fysieke drager, zoals papier, een cd/dvd-rom of een memory stick. Niet fysieke overdracht gaat bijvoorbeeld via e-mail, internet of fax.

2 Gegevens aanvrager (exporteur)

Vul hier de gegevens in van de aanvrager (exporteur). Dit is de natuurlijke persoon of rechtspersoon die de aanvraag doet of laat doen.

2b Relatiecode CDIU
Doet u een melding of aanvraag bij de CDIU? Dan krijgt u een relatiecode. Vul deze code hier in als u eerder een aanvraag of melding hebt gedaan.

2c EORI-nummer
Vul hier uw EORI-nummer in. Dit nummer bestaat uit uw RSIN/fiscaal nummer met een aanvulling. Hebt u nog geen EORI-nummer? Vul dan uw RSIN/fiscaal nummer in.

3 Gegevens agent/vertegenwoordiger

Vul hier de gegevens in van de agent/vertegenwoordiger die de aanvraag indient voor de exporteur (als dat van toepassing is). CDIU kan vragen om een schriftelijke volmacht waaruit blijkt dat de agent/vertegenwoordiger hiervoor toestemming heeft van de exporteur. In geval van vertegenwoordiging stuurt CDIU de vergunning naar de vertegenwoordiger.

3b Relatiecode CDIU
Vul hier de CDIU-relatiecode in van de agent/vertegenwoordiger.

3c EORI-nummer
Vul hier hier het EORI-nummer van de agent/vertegenwoordiger in.

4 Gegevens geadresseerde

Vul hier de gegevens in van de persoon of het bedrijf waar u de goederen naartoe stuurt.

5 Gegevens eindgebruiker

Vul hier de gegevens in van de eindgebruiker van de goederen (als dit een ander bedrijf of een andere persoon is dan de geadresseerde).

6 Individuele of globale vergunning

6a
Geef hier aan of u een globale of een individuele vergunning aanvraagt. Zie voor meer informatie de rubriek 'Gebruiksaanwijzing' bovenaan dit formulier.

6b Uiterste datum van uitvoer
Vul hier de maand in waarin naar verwachting alle goederen zijn geleverd.

7 Goederen

7a Omschrijving van de goederen
Vermeld hier de naam van de goederen die in Nederland gebruikelijk is. Vermeld ook bijzonderheden als deze van belang zijn voor het indelen van de goederen volgens de 'goederennaamlijst internationale handel'. Wees zo specifiek mogelijk, zodat duidelijk is om welke goederen het precies gaat.

7c Omschrijving van de goederen voor publicatie op de website van de overheid
Gebruik hierbij geen merknamen, geen type-aanduidingen of andere informatie waaruit de exporteur te herleiden is.

7d
- GN-code. Vul hier de GN-code in voor de goederen. Het gaat hier om het zogenoemde gebruikstarief. U vindt de GN-codes op de website van de Douane: gebruikstarief.douane.nl.
- CAS-nummer. Gaat het om chemicaliën? Vul dan hier het CAS-nummer in, het registratienummer van de Chemical Abstracts Service.
- SG-post. Vul hier het post-/categorienummer in. U vindt dit nummer in:
  - de 'Gemeenschappelijke EU-lijst van militaire goederen'
  - bijlage 1 van Verordening (EG) nr. 428/2009 van de Raad, van 5 mei 2009
  - bijlage III van Verordening (EG) nr. 1236/2005 van de Raad, van 27 juni 2005
  - de betreffende sanctieregeling

Wilt u goederen uitvoeren die vallen onder bijlage III van de verordening (EG) nr. 1236/2005? Vul dan het postnummer van de goederen in zoals dat in deze bijlage staat.

Wilt u goederen uitvoeren die vallen onder een bepaalde sanctieregeling? Vul dan in:
- het nummer van de bijlage waarop deze goederen voorkomen
- het postnummer goederen

8 Eindgebruik

Beschrijf het eindgebruik van de goederen zo specifiek mogelijk, zodat duidelijk is waarvoor de goederen precies gebruikt worden. Gebruik bijvoorbeeld niet 'metaalindustrie', maar 'frezen van roestvrijstalen buizen van ten behoeve van de scheepsbouw'.

Beschrijf het eindgebruik van de goederen voor publicatie op de website van de overheid. Gebruik hierbij geen merknamen, geen type-aanduidingen, of andere informatie waaruit de exporteur te herleiden is.

9 Transactie

9a
- Land van herkomst. Vul hier het land in vanwaar de goederen zijn verzonden met als bestemming Nederland, ongeacht de landen die tijdens het vervoer zijn aangedaan.
- Land van bestemming. Vul hier het land in waar de goederen naartoe worden verzonden.
- Lidstaat waar de goederen zich bevinden. Vul hier het land in waar de goederen zich op dit moment bevinden.
- Land van eindbestemming. Vul hier het land in waar het uiteindelijke eindgebruik plaatsvindt. U hoeft niet de landen te vermelden waar de goederen tijdens het vervoer door komen. Weet u dat de goederen uiteindelijk worden doorgeleverd aan een andere bestemming dan het land van eindbestemming? Dan moet u dit vermelden vak 9d 'Aanvullende informatie'.

9b Soort transactie
Kruis aan om welke soort transactie het gaat.

10 Afgiftevorm vergunning

Geef hier aan in welke vorm u de vergunning wilt hebben.

11 Ondertekening

Dient u de aanvraag schriftelijk in? Dan moet u of uw vertegenwoordiger de aanvraag ondertekenen.

U (aanvrager) of uw vertegenwoordiger verklaart met het ondertekenen en opsturen (schriftelijk) of het indienen (digitaal) van deze aanvraag:
- dat hij voor deze transactie geen tweede aanvraag heeft ingediend in een andere lidstaat
- dat hij weet dat de goederen in rubriek 7 strategische goederen zijn en dat het daarom van groot belang is de bestemming van de uit te voeren goederen juist aan te geven, en dat hij:
  - vóór hij de uitvoervergunning krijgt (als dat van toepassing is) een buitenlands document moet overleggen waaruit de eindbestemming van de uitgevoerde goederen blijkt
  - als hij de uitvoervergunning krijgt, de goederen alleen zal leveren aan de in de vergunning genoemde geadresseerde of eindgebruiker en dat hij de goederen niet zal uitvoeren als hij reden heeft om aan te nemen dat de goederen de geadresseerde of eindgebruiker niet zullen bereiken

10 2 e [redacted]

Van: namens Vergunningen
Aan: CDIU.VOORSTEL@BELASTINGDIENST.NL
Onderwerp: RE: 10 2 g [redacted] W de Wereld muv bad guy landen

II. BESLISSING IB/IMH

Beslissing : Vervallen
Naam : 10 2 e [redacted]
Datum : 19-07-2012
Handtekening :

Condities : Het bedrijf is op 13/7 bij EL&I op bezoek geweest. Aldaar besproken dat het bedrijf een nieuwe aangepaste aanvraag in gaat dienen.

Voorgelegd AIVD/POSS: J[ ] / N[x]

9

30