PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Certification report 2004/19

NEC V-WAY 64 V3.0 (µPD79216000) microcontroller

Courtesy Translation

Warning

This report is designed to provide principals with a document enabling them to certify the level of security offered by a product under the conditions of use or operation laid down in this report for the version evaluated. 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 user and administration guides evaluated, as well as with the product security target, which presents threats, environmental scenarios and presupposed 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 in and of itself a product recommendation from the certifying organization, and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

This report is a “courtesy translation” of the document “Rapport de certification 2004/19”.

Contents

Introduction

Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated 18 April, 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 fulfill 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 ITSEC and Common Criteria certification procedures have been published and are available in French on the following Internet site:

www.ssi.gouv.fr

Certificate Recognition Arrangement

The SOG-IS European **Recognition Arrangement** of 1999 enables all the Nations which have signed the agreement[1] to recognize the certificates issued by their certifying authority. Certificates recognized within the framework of this agreement are issued with the following label:

The central information system security department also signs **recognition agreements** with approved foreign organizations whose head offices are located outside the Member States of the European Community. These agreements may allow for certificates issued by France to be recognized by the signatory countries. They may also stipulate that certificates issued by any one party are to be recognized by all parties. The recognition of certificates may also be limited to a predetermined assurance level.

[1] As of April 1999, the following countries had signed the SOG-IS agreement: the United Kingdom, Germany, France, Spain, Italy, Switzerland, the Netherlands, Finland, Norway, Sweden and Portugal.

The Common Criteria Recognition Arrangement enables the nations that have signed the agreement[1] to recognize certificates issued within the framework of the Common Criteria program up to assurance level EAL4, with specific assurance components where applicable. Certificates recognized within the framework of this agreement are issued with the following label:

The following table presents the web sites of the national certification organizations of the countries which have signed the Common Criteria Recognition Arrangement:

Country	Certifying organization	Web site
France	DCSSI	www.ssi.gouv.fr
United Kingdom	CESG	www.cesg.gov.uk
Germany	BSI	www.bsi.bund.de
Canada	CSE	www.cse-cst.gc.ca
Australia-New Zealand	AISEP	www.dsd.gov.au/infosec
United States	NIAP	www.niap.nist.gov
Japan	IPA	www.ipa.go.jp

[1] As of November 2003, the following certificate-issuing countries had signed the agreement: France, Germany, the United Kingdom, the United States, Canada , Australia-New Zealand and Japan; the countries which do not issue certificates but which have signed the agreement are: Spain, Finland, Greece, Israel, Italy, Norway, the Netherlands, Sweden, Austria and Turkey.

1. Evaluated product

1.1. Product identification

The product subject to the evaluation is the microcontroller developped by NEC referenced NEC V-WAY 64 V3.0 (µPD79216000) microcontroller. This microcontroller embeds a test software as well as two software libraries, which are delivered in an object format (linkable), as follows:

- The interface library to access the cryptoprocessor hardware (Licrypt.a version 3.0),
- The RSA calculation library (RSAlib.a version 2.0).

The reference of the certified product is: V01005V30054 mnnn vw; where mnnn identifies software code USER ROMCODE and TEST ROMCODE, and vw identifies the test programme.

1.2. Product Developper

The product was developed and manufactured by several entities within NEC Electronics group (cf. Product life cycle §1.3.2), as follows:

The product was developed and tested by:

NEC Electronics Europe, Smart Card Application Center

4, avenue Morane Saulnier
78140 Vélizy
France.

NEC Micro Systems (Kumamoto)

2081-24 Tabaru Michiki-machi
Kamimashiki-gun
Kumamoto 861-2202
Japan

The photo masks of the microcontroller were produced by:

Toppan printing Ltd

7-21-33 Nobidome Niiza-city
Saitama 352-8562
Japan

The wafer production was performed by:

NEC Electronics Sagamihara

1120 Shimokusawa Sagamihara-city
Kanagawa 229-1198
Japan

The production tests and the wafer sawing operations were performed by:

NEC Yamaguchi

192-3 Kamimoto, Higashimagura,
Kusunoki-cho, Asa-gun,
Yamaguchi 757-0298,
Japan

1.3. Product Description

The product subject to the evaluation is the NEC V-WAY 64 V3.0 microcontroller.

This product features two modes of operation:

- **«Test» mode:** Upon the completion of its production, the microcontroller is being tested thanks to an external testing system and the internal test software embedded in the ROM of the device. Once those tests are completed the prepersonalization data are stored in the appropriate EEPROM area and the microcontroller is locked into «User Mode» in a Non-reversible manner.
- **«User» mode:** This mode is the final mode of utilization for the microcontroller. It then operates under the control of the software, which is embedded on the Smart Card. Accessing the test software in the user mode is absolutely impossible; thus the «User» mode is the unique mode available to the final users.

The microcontroller cannot be used as such, without embedded software. Together with its appropriate operating system software, the microcontroller is designed to host one or more applications. Inserted as a module in a plastic card, the microcontroller will be a key element of the so called Smart Card. Potential applications are ranging from Banking to Pay TV, Transportation or health card depending on the embedded application software. These pieces of software are not in the scope of the evaluation described herein.

1.3.1. Architecture

The V-Way64 Microcontroller is based on a 0,25µm CMOS technology and provides the following features:

- Hardware part:
  - 32-bit RISC CPU;
  - Memory configuration: 200 KB of ROM (192 KB USER_ROM, 8 KB TEST_ROM), 64 KB of EEPROM, 64 Bytes of OTP ROM, a set of special registers for User and Test modes, 4 KB of RAM;
  - Cryptography processing unit (NEC SuperMAP),
  - DES hardware accelerator;
  - 36 MHz on chip clock system;
  - 16 bit Random Number Generator;
  - Two 16 bit Timers;
  - Interrupt controller (49 input);

- ISO7816 & EMV compliant serial interface unit;
- Full set of security mechanisms;
- Stand-by controller (HALT, IDLE, STOP modes);
- Power management unit including a Reset generator and a Voltage regulator;

▪ Software part:

- The interface library to access the hardware cryptoprocessor;
- The RSA calculation library;
- The microcontroller test and evaluation software.

A detailed description of the architecture is available in the [HLD] documentation.

1.3.2. Life Cycle

The product life cycle derives from the life cycle described under PP/9806 [PP9806] as follows :

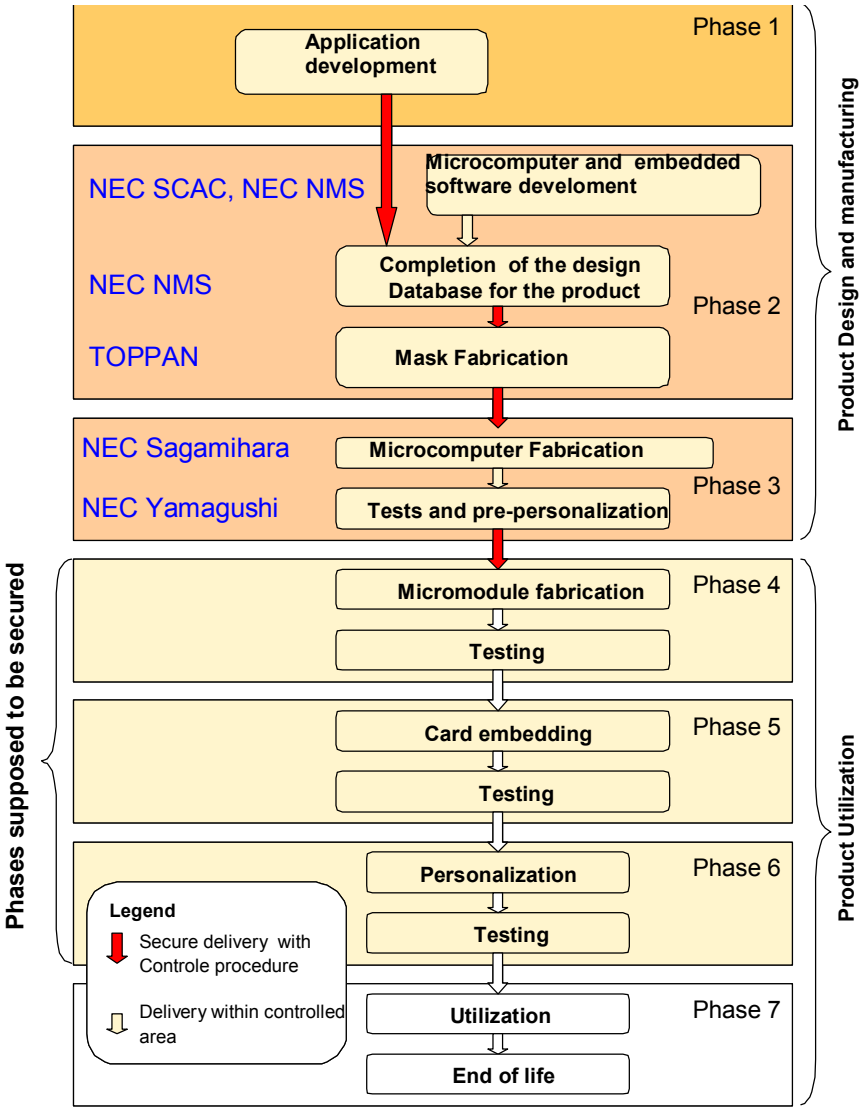

Figure 1 – Standard Smart Card life cycle

1.3.3. Scope of the product evaluation

This certification report presents the evaluation work on the V-Way64 Microcontroller and its associated software libraries as described under section 1.3.1. Any other embedded application, including those, which were embedded for the sole purpose of the evaluation work, are not in the scope of this evaluation.
With reference to the life cycle here above, the evaluated product is the one coming out of phase 3 consisting in the microcontroller fabrication, testing and pre-personalization.

1.4. Utilization and administration

1.4.1. Utilization

The evaluated product is not embedding any particular application. It consists in a hardware and software platform offering various services for embedded software to be used in Smart Card applications. In fact there is no real utilization of the microcontroller as such. The users of the microcontroller can be seen as the application developers as well as all bodies involved in the so called administration phases of the micromodule and the card (phase 4 to 6) where embedded applications are configured and personalized.

Within the V-WAY64 V3.0 evaluation, users are being defined as those who can actually implement the functionalities of the microcontroller as described under section 1.3.1.

This definition includes all users having access to the product in « user » mode including the card issuer, the developer of embedded software, bodies in charge of card embedding or card integration within its complete system.

The security objectives related to the design environment and the final use of the product are listed in the security target [ST].

1.4.2. Administration

The phases 4 to 6 of the product life cycle (so called administration phases) are covered by an assumption within the protection profile, that those phases are realized in the appropriate conditions, which would not jeopardize the security of the product. Those conditions have not been investigated in the context of this evaluation.

2. The evaluation

2.1. Evaluation facility

CEACI (Thalès Microelectronics – CNES)

18, avenue Edouard Belin
31401 Toulouse Cedex 4
France

Phone : +33 5 61 27 40 29

E-mail address : ceaci@cnes.fr

The evaluation has been carried out from September 2002 to March 2004.

2.2. Sponsor

NEC Electronics (Europe) GmbH
Smart Card Application Center

9, rue Paul Dautier
B.P. 52
78142 Vélizy Cedex
France

2.3. Evaluation criteria

The evaluation has been carried in compliance with Common Criteria [CC], and with the evaluation methodology described in CEM [CEM] including final interpretations listed in the evaluation reports.

2.4. Security target evaluation

The security target [ST] defines the evaluated product and its operational environment.
All security functional requirements and security assurance requirements from the security target are taken from part 2 and part 3 of Common Criteria [CC].
The security target meets ASE class requirements.

2.5. Product evaluation

The evaluation consists in checking that the product and its documentation are compliant to security functional and assurance requirements defined in the security target [ST] of the product.

2.5.1. Product development

ADV assurance class – development – defines requirements for the stepwise refinement of the product's security functions from its summary specification in the security target [ST] down to the actual implementation. Each of the resulting product's security function representations

provide information to help the evaluator determine whether the functional requirements of the product have been met.
Documents associated to ADV class analysis shows that security functional requirements are correctly and completely refined into the different levels of the product representation (functional specifications (FSP), subsystems (HLD), modules (LLD) and implementation (IMP)), down to the implementation of its security functions.
Documents provided for ADV – development – class evaluation meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.2. Documentation

From the point of view of the evaluation, there is no administrator of the micro-controller during the usage phases (4 to 7 of the lifecycle). Indeed, administration of these phases are linked to a specific application that is not include in the evaluation perimeter. The users are considered to be the persons that can operate the functionalities of the product (e.g. the embedded software developer).
User guides [USR] and administrator guides [IGS] meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.3. Delivery and installation

According to the evaluation guidance « The application of CC to IC » [CC_IC], delivery is considered:

- delivery of embedded software code to the developer of micro-controller,
- delivery of required information to the mask developer,
- delivery of the mask to the micro-controller developer,
- delivery of the micro-controllers to the person in charge of the next step (embedding…).

The various sites involved are identified in §1.2 of this report. Within the evaluation, visits have been carried out on these sites to verify that the procedures are applied (cf. Annex 1 to 5).
The delivery [DEL] procedure is sufficient to fulfil the requirements: it permits to identify the origin of the delivery and to detect any modification of the product during its delivery.
The product start-up is a RESET, the installation, generation and start-up procedures [IGS] permit to have a secure configuration of the product.
Documents provided for ADO – Delivery and operation – class evaluation meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.4. Development environment

The configuration management system is used according to the configuration plan [ACM].
The configuration list [LGC] identifies the elements traced by the configuration management system. The configuration elements identified in the configuration list are maintained by the configuration management system. The procedures for generating the product are sufficient to ensure that correct configuration elements are used to generate the product.
The various sites involved in the development of the product are identified at §1.2 in this report.
Security measures described in procedures provide the sufficient level of protection to maintain the confidentiality and the integrity of the evaluated product and its documentation.

The evaluator checked that procedures are followed in a manner consistent with that described in the development and configuration management documentation. Sites visits have been performed [Visit].
Documents provided for ALC – Lifecycle support – class evaluation meet requirements from part 3 of Common Criteria [CC] in term of form and content of evidence.

2.5.5. Functional testing

The evaluator checked that all security functions and functional specification interfaces of the product are mapped to at least a functional test described in the test documentation. He checked also that all security functions, as described is the high-level design documentation [HLD], are covered by the developer tests.

2.5.6. Vulnerability assessment

Vulnerabilities identified by the developer have been checked through an analysis and through penetration testing. The evaluator concludes that vulnerabilities identified by the developer are correctly covered.
The evaluator performed an independent vulnerability analysis that results do not point out any additional vulnerability.
The product within its operational environment is resistant to an attacker possessing a **high** level attack potential.

3. Conclusions of the evaluation

3.1. Evaluation technical report

The Evaluation Technical Report [RTE] describes results from the evaluation of NEC V-WAY 64 V3.0 (µPD79216000) microcontroller.

3.2. Evaluation level

NEC V-WAY 64 V3.0 (µPD79216000) microcontroller has been evaluated in compliance to Common Criteria [CC] and its methodology [CEM] at level EAL4[1] augmented with following assurance components, compliant to Common Criteria part 3:

Components	
ADV_IMP.2	Implementation of the TSF
ALC_DVS.2	Sufficiency of security measures
AVA_VLA.4	Highly resistant

Tableau 1 - Augmentations

For all these product evaluation level components, following verdicts have been issued:

Class ASE	Security Target evaluation	Verdict
ASE_DES.1	TOE description	Pass
ASE_ENV.1	Security environment	Pass
ASE_INT.1	ST introduction	Pass
ASE_OBJ.1	Security objectives	Pass
ASE_PPC.1	PP claims	Pass
ASE_REQ.1	IT security requirements	Pass
ASE_SRE.1	Explicitly stated IT security requirements	Pass
ASE_TSS.1	Security Target, TOE summary specification	Pass
Class ACM	**Configuration management**	
ACM_AUT.1	Partial CM automation	Pass
ACM_CAP.4	Generation support and acceptance procedures	Pass
ACM_SCP.2	Problem tracking CM coverage	Pass
Class ADO	**Delivery and operation**	
ADO_DEL.2	Detection of modification	Pass
ADO_IGS.1	Installation, generation, and start-up procedures	Pass

[1] In Appendice 7, a table gives a brief description of existing Evaluation Assurance Levels (EAL) defined in Common Criteria [CC].

Class ADV	**Development**	
ADV_FSP.2	Fully defined external interfaces	Pass
ADV_HLD.2	Security enforcing high-level design	Pass
ADV_IMP.2	Implementation of the TSF	Pass
ADV_LLD.1	Descriptive low-level design	Pass
ADV_RCR.1	Informal correspondence demonstration	Pass
ADV_SPM.1	Informal TOE security policy model	Pass
Class AGD	**Guidance**	
AGD_ADM.1	Administrator guidance	Pass
AGD_USR.1	User guidance	Pass
Class ALC	**Life cycle support**	
ALC_DVS.2	Sufficiency of security measures	Pass
ALC_LCD.1	Developer defined life-cycle model	Pass
ALC_TAT.1	Well-defined development tools	Pass
Class ATE	**Tests**	
ATE_COV.2	Analysis of coverage	Pass
ATE_DPT.1	Testing: high-level design	Pass
ATE_FUN.1	Functional testing	Pass
ATE_IND.2	Independent testing - sample	Pass
Class AVA	**Vulnerability assessment**	
AVA_MSU.2	Validation of analysis	Pass
AVA_SOF.1	Strength of TOE security function evaluation	Pass
AVA_VLA.4	Highly resistant	Pass

Tableau 2 – Components and their corresponding verdicts

3.3. Functional requirements

The product meets the following security functional requirements [ST chapter 5] :

- Potential violation analysis (FAU_SAA.1)
- Cryptographic operation (FCS_COP.1)
- Complete access control (FDP_ACC.2)
- Security attributes based access control (FDP_ACF.1)
- Subset information flow control (FDP_IFC.1)
- Simple security attributes (FDP_IFF.1)
- Stored data integrity monitoring and action (FDP_SDI.1)
- User attribute definition (FIA_ATD.1)
- User authentication before any action (FIA_UAU.2)
- User Identification before any action (FIA_UID.2)
- Management of security functions behaviour (FMT_MOF.1)
- Management of security attributes (FMT_MSA.1)
- Static attribute initialisation (FMT_MSA.3)
- Security management roles (FMT_SMR.1)

- Unobservability (FPR_UNO.1)
- Notification of physical attack (FPT_PHP.2)
- Resistance to physical attack (FPT_PHP.3)
- TOE Security Functions testing (FPT_TST.1)

3.4. Strength of functions

Only authentication functions have been subject to an estimation of their strength.
Strength of security functions meets the **high level (SOF-high).**

3.5. Cryptographic mechanisms analysis

Only the random generator has been analysed in a cryptographic scope during this evaluation (cf annex 2).

3.6. Protection profile claim

This product is compliant with the requirements of PP/9806 [PP9806].

3.7. European recognition (SOG-IS)

This certification report is emited within the requirement of the SOG-IS [SOGIS] recognition agreement with the disponibility of a security target [ST].

3.8. International recognition (CC RA)

This certification report is emited within the requirement of the CC-RA recognition agreement with the disponibility of a security target [ST].
The following augmentations above EAL4 are not recognise within CC-RA [CCRA]: ADV_IMP.2, ALC_DVS.2 and AVA_VLA.4 (Tableau 1).

3.9. Usage restrictions

Operational environment have to respect security objectives for the environment (§ 3.10), as well as recommendations within user guidance [USR] and administrator guidance | IGS].
Results from the evaluation are valid only for the configuration specified in this certification report.
This certification report gives an assessment on the strength of the "NEC V-WAY 64 V3.0 (µPD79216000) microcontroller" to resist to attacks, these attacks remain generic as no specific application is embedded. Therefore, the security of a complete product built on this microcontroller will only be assessed with the evaluation of the complete product; the complete evaluation can be based on the results of this evaluation.

3.10. Security objectives for the environment

Security objectives for the environment are the followings [ST § 4.2.6], they apply to the system that uses the microcontroller with its embedded application:

- Secure communication protocols and procedures shall be used between smartcard and terminal.

- The integrity and the confidentiality of sensitive data stored/handled by the system (terminals, communications…) shall be maintained.

3.11. Result summary

The whole evaluation work performed by the evaluation centre is accepted by the certification body who testify that NEC V-WAY 64 V3.0 (µPD79216000) microcontroller identified in paragraph 1.1 and described in paragraph 1.3 of this report is compliant with requirements specified into the security target [ST]. The whole evaluation work and theirs results are described within the evaluation technical report [RTE].

Appendice 1. Report of the site visit : NEC in Vélizy

The following NEC site in charge of the development and the test of the product:

NEC Electronics Europe, Smart Card Application Center

4, avenue Morane Saulnier
78140 Vélizy
France

was subject of a site visit in **December 2003,** in the context of the V-WAY64 V3.0 evaluation, in order to verify its conformance with the evaluation criterias and the documentation concerning:

- The configuration management: **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- The deliveries: **ADO** (ADO_DEL.2) ;
- The development security: **ALC** (ALC_DVS.2).

The visit by the evaluation body together with an attendant from the DCSSI, resulted in positive conclusions as to the required criterias for the site.

Appendice 2. Report of the site visit : NEC in Kumamoto

The following NEC site in charge of the development and the test of the product:

NEC Micro Systems (Kumamoto)

2081-24 Tabaru Michiki-machi
Kamimashiki-gun
Kumamoto 861-2202
Japan

was subject of a site visit in **October 2003,** in the context of the V-WAY64 V3.0 evaluation, in order to verify its conformance with the evaluation criterias and the documentation concerning:

- The configuration management: **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- The deliveries: **ADO** (ADO_DEL.2) ;
- The development security: **ALC** (ALC_DVS.2).

The visit by the evaluation body resulted in positive conclusions as to the required criterias for the site.

Appendice 3. Report of the site visit : NEC in Sagamihara

The following NEC site in charge of the wafer fabrication:

NEC (Sagamihara)

1120 Shimokusawa Sagamihara-city
Kanagawa 229-1198
Japan

was subject of a site visit in **October 2003,** in the context of the V-WAY64 V3.0 evaluation, in order to verify its conformance with the evaluation criterias and the documentation concerning:

- The configuration management: **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- The deliveries: **ADO** (ADO_DEL.2) ;
- The development security: **ALC** (ALC_DVS.2).

The visit by the evaluation body resulted in positive conclusions as to the required criterias for the site.

Appendice 4. Report of the site visit : NEC in Yamaguchi

The following NEC site in charge of the wafer testing and sawing:

NEC (Yamaguchi)

192-3 Kamimoto, Higashimagura,
Kusunoki-cho, Asa-gun,
Yamaguchi 757-0298,
Japan

was subject of a site visit in **October 2003,** in the context of the V-WAY64 V3.0 evaluation, in order to verify its conformance with the evaluation criterias and the documentation concerning:

- The configuration management: **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- The deliveries: **ADO** (ADO_DEL.2) ;
- The development security: **ALC** (ALC_DVS.2).

The visit by the evaluation body resulted in positive conclusions as to the required criterias for the site.

Appendice 5. Report of the site visit : Toppan in Tokyo

The following NEC site in charge of the photo masks fabrication:

Toppan printing Ltd

7-21-33 Nobidome Niiza-city
Saitama 352-8562
Japan

was subject of a site visit in **October 2003,** in the context of the V-WAY64 V3.0 evaluation, in order to verify its conformance with the evaluation criterias and the documentation concerning:

- The configuration management: **ACM** (ACM_AUT.1, ACM_CAP.4) ;
- The deliveries: **ADO** (ADO_DEL.2) ;
- The development security: **ALC** (ALC_DVS.2).

The visit by the evaluation body resulted in positive conclusions as to the required criterias for the site.

Appendice 6. Cryptographic mechanisms analysis

The NEC V-WAY 64 V3.0 (µPD79216000) microcontroller provides a random numbers generator.

This service is to be used by an embedded application and has been analysed by DCSSI. The analysis shows that in the case this random number generator shall be used for cryptographic means, it has to be used in compliance with the guidance [USR].

Appendice 7. Evaluation Assurance Levels ISO 15408 or CC

Class	Family	Components by assurance level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ACM class Configuration management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
ADO class Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
ADV class Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
AGD class Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
ALC class Life cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
ATE class 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**
AVA class 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

Appendice 8. Evaluated product documentation

[ACM]	Configuration Management Smartcard Manual, réf: 81-00U0-00001, version 1.30 of 9/09/2003.
[Visite]	• Visit Report ARSIA (NEC SCAC Vélizy), réf: ARS_RDV_SCAC, version 1.0 of 12/12/2003; • ARSIA Audit Site : NEC NMS / Kumamoto October 01st & 02nd, 2003, réf: ARS_RDV_NMS, version a; • ARSIA Audit Site : Toppan Printing / Tokyo September 30th, 2003, réf: ARS_RDV_TOP, version a; • ARSIA Audit Site : NEC UC line + G4/ Sagamihara October 06th 2003, réf : ARS_RDV_SAG, version a; • ARSIA Audit Site : NEC / YAMAGUCHI October 01st & 02nd, 2003, réf: ARS_RDV_YAM, version a.
[DEL]	ADO_DEL: Delivery of the TOE, réf: 81-55w1-00001, version 1.01 of 13/01/2004.
[HLD]	Total Chip (TC) High Level Design, réf: 33-55Q1-10000, version 1.04 of 29/03/2004.
[IGS]	V-WAY64-V 3.0 [uPD79216000] Installation, Generation and Start-Up, réf 33-55F1-10000, version 1.10 of 12/11/2003.
[LGC]	VWAY 64 Configuration List, réf: 33-55U1-00001, version 1.04 of 26/04/2004. VWAY 64-V3.0 EAL4+ Document Navigator, réf: 33-5511-10002, version 1.23 of 17/06/2004.
[RTE]	Evaluation Technical Report of ARSIA project, réf: ARS_ETR, version 1.0 of 29/04/04.
[ST]	µPD79216000 V3.0 (V-WAY 64 V3.0) Security Target, Ref:33-55N1-10000, version 1.34 of 31/03/2004. µPD79216000 V3.0 (V-WAY 64 V3.0) Security Target Lite, Ref:33-55N1-10001, version 1.00 of 12/07/2004.
[USR]	V-WAY 64-V 3.0 [uPD79216000] User Guidance, réf: 33-65K1-10000, version 1.02 of 26/04/04.
[PP9806]	Common Criteria for Information Technology Security Evaluation - Protection Profile : Smart Card Integrated Circuit Version 2.0, Issue September 1998. Certified by the French certification body under reference PP/9806.

Appendice 9. Certification references

Decree 2002-535 of 18 April 2002 relating to evaluation and certification of security provided by information technology products and systems.	
[CC]	Common Criteria for Information Technology Security Evaluation: • Part 1: Introduction and general model, version 2.1, August 1999; • Part 2: Security functional requirements, version 2.1, August 1999; • Part 3: Security assurance requirements, version 2.1, August 1999.
[CEM]	Common Methodology for Information Technology Security Evaluation: • Part 2: Evaluation Methodology, version 1.0, August 1999.
[IS 15408]	Information technology — Security techniques — Evaluation criteria for IT security: • ISO/IEC 15408-1:1999(E): Part 1: Introduction and general model; • ISO/IEC 15408-2:1999(E): Part 2: Security functional requirements; • ISO/IEC 15408-3:1999(E): Part 3: Security assurance requirements.
[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.

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
Bureau certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP
France

certification.dcssi@sgdn.pm.gouv.fr