Certification Report

EAL 2+ Evaluation of Diversinet Passport Certificate Serverâ

Version 4.1.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-9
Version:	1.0
Date:	10 May 2002
Pagination:	i to iii, 1 to 9

DISCLAIMER

The information technology (IT) product identified in this certification report, and associated certificate, has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Evaluation and Certification Scheme using the Common Methodology for Information Technology Security Evaluation, Version 1.0, for conformance to the Common Criteria for IT Security Evaluation, Version 2.1. This certification report, and associated certificate, applies only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Evaluation and Certification Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and associated certificate, is not an endorsement of the IT product by the Communications Security Establishment (CSE) or by any other organization that recognizes or gives effect to this report, and associated certificate, and no warranty of the IT product by the CSE or by any other organization that recognizes or gives effect to this report, and associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (Canadian CCS) provides a third-party evaluation service for determining the trustworthiness of IT security products. Evaluation is performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Canadian CCS Certification Body (CB), managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has demonstrated the ability to meet the requirements of the Canadian CCS CB for approval to perform Common Criteria evaluations. A significant requirement for such approval by the Canadian CCS CB is accreditation to the requirements of the *ISO Guide 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN) administered by the Standards Council of Canada.

The CCEF who performed the evaluation of Diversinet Passport Certificate Server® version 4.1.1 was DOMUS IT Security Laboratories, IBM CANADA LIMITED, located in Ottawa, Ontario, Canada.

By awarding a certificate, the CB asserts that a product complies with the security requirements specified in its Security Target (ST). A ST is a requirement specification document that defines and scopes the evaluation activities. The consumer of certified IT products should review the ST, in addition to the Certification Report (CR), in order to gain an understanding of any assumptions made during evaluation, the IT product's intended environment, its security requirements, and the level of confidence (evaluation assurance level) that the product satisfies its security requirements.

The ST associated with this CR is identified by the following nomenclature:

Security Target Document
Passport Certificate Server Ver. 4.1.1
Common Criteria EAL 2 (augmented)
Version 1.00
Dated: 30 April 2002

This CR is associated with the Certificate of Product Evaluation dated 10 May 2002. Both the ST and CR are posted on the Canadian Certified Product List.

Oracle 8i® database is a registered trademark of Oracle®. Windows NT® is a registered trademark of Microsoft Corporation. Diversinet Passport Certificate Server® is a registered trademark of Diversinet Corp. RSA BSAFE® is a registered trademark of RSA Security.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Diversinet Passport Certificate Server® version 4.1.1, from Diversinet Corp., is the Target of Evaluation (TOE) for this EAL 2 augmented evaluation. The Diversinet Passport Certificate Server® provides system developers with a secure PKI capable of creation, management, and retirement of public key certificates, suitable for a wireless PKI. The main security functionality of the TOE is to provide secure management of certificates.

The Passport certificate format supports a number of user-selectable algorithms; however, in this evaluation, all public-key cryptography was performed using the RSA algorithm. The cryptography is provided by the RSA BSAFE® module version 4.3.1. This module has undergone a FIPS 140-1 validation under the Cryptographic Module Validation Program and was awarded certificate #89.

The threats that are countered by the Diversinet Passport Certificate Server® include: attempts to masquerade as an authorized user, replay of authentication data, attempts to repudiate communication, unauthorised use of keys, attempts by users to gain privileges they are not entitled to, and eavesdropping on communications.

DOMUS IT Security Laboratories, IBM Canada Limited was the Common Criteria Evaluation Facility that conducted the evaluation. The evaluation was completed on 26 March 2002. The evaluation was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme.

The scope of the evaluation is defined by the ST, which identifies assumptions made during the evaluation, the IT product's intended environment, the security requirements, and the level of confidence (evaluation assurance level) that the product satisfies its security requirements. Consumers of Diversinet Passport Certificate Server® are advised to verify that their own environment is consistent with the ST, and to give due consideration to the comments, observations and recommendations in this Certification Report.

The results documented in the Evaluation Technical Report for this product indicate that the product meets the EAL 2 augmented assurance requirements for its evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*. The Diversinet Passport Certificate Server® version 4.1.1 has been found to be Common Criteria Part 2 and Part 3 conformant, containing only functional requirements from Part 2 and only assurance requirements from Part 3.

The Communications Security Establishment, as the Canadian Common Criteria Evaluation and Certification Scheme Certification Body, declares that the Diversinet Passport Certificate Server® version 4.1.1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the Certified Products List.

1 Identification of Target of Evaluation

The scope of this evaluation is the Diversinet Passport Certificate Server® version 4.1.1. The platform for the Diversinet Passport Certificate Server® is Microsoft Windows NT® 4.0 with Service Pack 5 or higher. All other components referred to in this document, though typically present in a deployment, are not covered by this evaluation and certification.

The Diversinet Passport Certificate Server® uses cryptographic functions – both symmetric and public-key – to provide security services that meet the requirements specified in the Security Target (ST). The Diversinet Passport Certificate Server® uses the RSA BSAFE® Crypto-C toolkit to provide those cryptographic functions.

2 Product Description

The Diversinet Passport Certificate Server® version 4.1.1 provides the infrastructure components for a secure wireless Public Key Infrastructure (PKI).

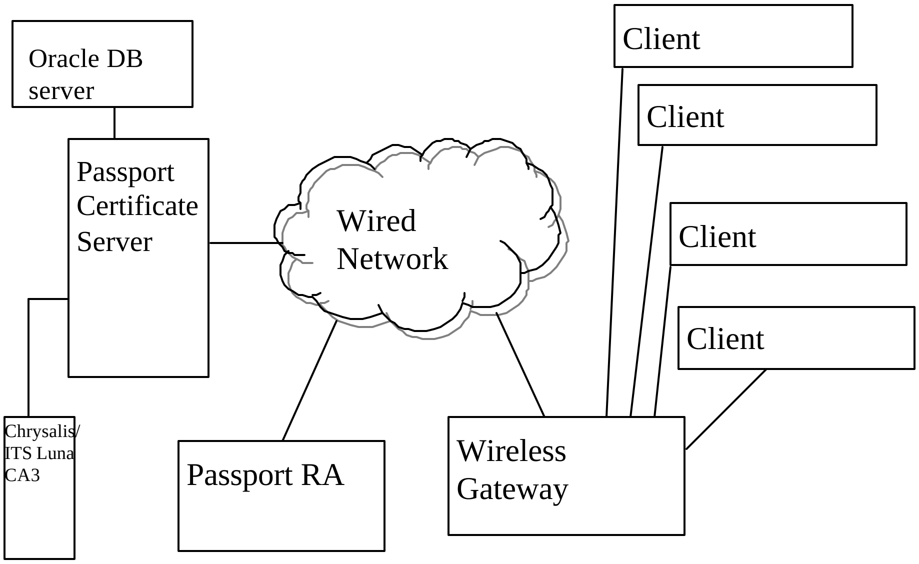

Figure 1: Typical Deployment of Passport Certificate Server®

The Diversinet Passport Certificate Server® version 4.1.1 is installed on a computer typically connected to a wired network, such as the Internet or a corporate intranet or extranet. Diversinet Passport Certificate Server® is supported by a database (typically Oracle 8i®) on the same or another computer; and a hardware cryptographic module (typically, the Chrysalis-ITS® Luna® CA^{3}), connected to the computer.

The Passport Registration Authority® is also typically connected to the same wired network as the Diversinet Passport Certificate Server®.

Clients are wireless, mobile devices such as cell phones, two-way pagers, or personal digital assistants that transmit and receive messages. Clients have software that uses the Diversinet specified certificate formats and protocol messages, allowing them to communicate with the Diversinet Passport Certificate Server® and the Passport Registration Authority®.

The Diversinet Passport Certificate Server® version 4.1.1 provides system developers with a secure PKI capable of creation, management and retirement of public key certificates. The format of these certificates is proprietary. The small size of the Diversinet Passport certificates is an advantage over the X.509 version 3 certificate format in embedded, high performance or constrained bandwidth systems.

3 Security Policy

The Diversinet Passport Certificate Server® security policy consists of four parts: an access control policy, an information flow policy, an identification/authentication policy, and an audit policy.

In the Diversinet Passport Certificate Server®, the access control policy governs the actions of Users, Administrators and the Security Officer on the User key pairs and the User certificates, collectively referred to as User IDs. Users can only access their own private keys. Users can lock their own IDs. Administrators can lock and unlock any User ID.

The Diversinet Passport Certificate Server® enforces an information flow policy that specifies all communications between client and server are:

- Authenticated between client and server;
- Encrypted for confidentiality; and
- Time-stamped and digitally signed for integrity.

The identification and authentication policy of the Diversinet Passport Certificate Server® only allows actions after successful authentication.

The audit policy for the Passport Certificate Server ® version 4.1.1 governs the generation, protection, review, and storage of audit records.

For further details on these security policies refer to section 2.5 of the ST.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

It is assumed for the purpose of this evaluation that the Diversinet Passport Certificate Server® users and administrators are trusted. The Diversinet Passport Certificate Server® should be installed using the secure installation procedures in the User's Guide and the Install Wizard. The secure configuration of the Diversinet Passport Certificate Server® is described in the User's Guide.

4.2 Environmental Assumptions

The Diversinet Passport Certificate Server® employs an Oracle 8i® database for certificate storage. This database must be available for the Diversinet Passport Certificate Server® to function. The physical security of the Diversinet Passport Certificate Server® and the level of trust in personnel using its services, are both assumed to be adequately handled in the environment to an appropriate level.

4.3 Clarification of Scope

The Diversinet Passport Certificate Server® operates in an environment that is assumed to be physically secure. The TOE does not counter threats related to compromise by a local user.

5 Architectural Information

There are 12 subsystem of the The Diversinet Passport Certificate Server® that perform the following tasks:

- The *main subsystem* initializes and terminates the other subsystems.
- The *console subsystem* handles requests from "console" applications that are run from the local server.
- The *listener subsystem* accepts incoming client connections, and passes them on to the worker pool subsystem.
- The *worker pool subsystem* services client requests. It maintains a pool of threads, each servicing requests from one client connection.
- The *crypto subsystem* provides encryption/decryption and signing/verifying services.
- The *database subsystem* loads and unloads the database module, opens database connections, and provides access (to the database connections) to other subsystems.
- The *license watchdog subsystem* ensures license compliance.
- The *logging subsystem* manages the log files (audit, general, and trace).
- The *nonce subsystem* generates and verifies server nonces.

- The *performance monitor subsystem* generates performance data for export to the Windows NT® Performance Monitor utility.
- The *root key manager subsystem* builds Certificate Root Update Structures as required.
- The *server certificate subsystem* provides access to the server certificate and verifies the server certificate key lock passphrase.

6 Evaluated Configuration

The minimum system requirements for the TOE are stated in the User's Guide. The evaluated configuration was the Diversinet Passport Certificate Server® Version 4.1.1 on the following platform:

- PC: IBM NetVista
- Operating System: Microsoft Windows NT® 4.0 Server Service Pack 5
- Oracle 8i® V.8.1.6

7 Documentation

The documentation for Diversinet Passport Certificate Server® version 4.1.1 is *Passport Certificate Server Version 4.1.1 User's Guide, June 2001.*

8 Evaluation Analysis Activities

The evaluation involved an analysis of the developer's processes used to develop and support the Diversinet Passport Certificate Server® and the associated documentation. The product documentation and design were considered from a security perspective along with the guidance documentation.

The evaluation analysis activities involved a structured evaluation of the product documentation in the following areas:

- Configuration Management (CM);
- Product Delivery and Operation, including secure installation and start-up;
- Development documentation (specifications, informal security policy model, design and requirements traceability);
- Guidance documentation;
- Testing (developer's coverage and functional testing);
- Strength of Function (for password mechanisms); and
- Vulnerability Assessment for the product.

An analysis and examination of the Diversinet Passport Certificate Server®, its development environment, and its associated CM documentation was performed.

The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when the Diversinet Passport Certificate Server® is delivered to the customer.

The evaluators examined the design documentation and determined that it describes the design and function of the product.

The evaluators examined the guidance documentation and determined that it describes how to securely use and administer the product.

The Diversinet Passport Certificate Server® Security Target's claims for the strength of function and the developer's vulnerability analysis were validated through independent evaluator analysis.

All activities for the evaluation of the Security Target and the evaluation of the Diversinet Passport Certificate Server® resulted in a PASS verdict. These verdicts resulted from evaluation activities performed at DOMUS IT Security Laboratories, IBM Canada Limited facilities in Ottawa, Ontario and a site visit conducted at Diversinet Corporation offices in Toronto, Ontario.

9 ITS product testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent vulnerability tests. During this evaluation the evaluators developed their independent tests by examining the design documentation, examining developer analysis, and repeating the full set of developer tests.

9.1 Testing coverage

The developer provided test documentation, which was comprised of a test suite and an analysis of coverage. As the developer had tested all of the security functions, the evaluator chose to augment the developer's tests by devising test scripts to explicitly test areas that had only been implicitly tested by the developer. The tests focused on the security functional requirements in the ST. The detailed prerequisites for the tests implicitly verified the installation procedures.

9.2 Vulnerability testing

A vulnerability test plan was devised using the Diversinet vulnerability assessment, the functional specification, the high-level design, the ST, the User's Guide, and the Install Wizard. These tests focused on network based vulnerabilities, since the Diversinet Passport Certificate Server® is deployed in a network.

9.3 Conduct of testing

All testing took place at DOMUS IT Security Laboratories, IBM Canada Limited and was subject to oversight by the CCS CB. To perform the testing the evaluator used public domain tools for analyzing network traffic and performing network attacks. The evaluator also used a developer supplied test tool and the product interface for functional testing. In addition, the evaluator created new attack scripts to assist in the vulnerability testing.

9.4 Results

The developer tests and independent functional tests yielded the expected results, giving assurance that the TOE behaves as specified in the ST and the design documentation. The vulnerability testing received a pass verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities of the Diversinet Passport Certificate Server® in its intended operating environment.

10 Results of the Evaluation

The evaluation of the Diversinet Passport Certificate Server® has determined that it is CC Part 2 conformant to the functional requirements defined in the ST and CC Part 3 conformant to EAL 2 augmented with ADV_SPM.1 *Informal TOE Security Policy Model*.

The evaluation demonstrated that the Diversinet Passport Certificate Server® provides the claimed security functions. The Diversinet Passport Certificate Server® uses cryptographic functions to provide security services that meet the requirements in the ST; these cryptographic functions are provided by the RSA BSAFE® Crypto-C toolkit. Note that RSA BSAFE® Crypto-C Toolkit version 4.3.1 has been awarded certificate #89 under the FIPS 140-1 Cryptographic Module Validation Program. This module meets FIPS 140-1 level 1 when running on Windows NT®.

This evaluation has provided the grounds for EAL 2+ level of assurance. These results and their supporting rationale are supported by evidence contained in the *Evaluation Technical Report* (ETR). The ETR is a document internal to the Canadian CCS that contains proprietary information, and is therefore not publicly available.

11 Evaluator Comments, Observations and Recommendations

The Diversinet Passport Certificate Server® must be configured as stated in the User's Guide and must be installed with at least the minimum system requirements on a Microsoft Windows NT® 4.0 Server operating system with Service Pack 5.

12 Glossary

This section expands upon abbreviations.

Abbreviation	Description
CB	Certification Body
CC	Common Criteria for IT Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CM	Configuration Management
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PKI	Public Key Infrastructure
ST	Security Target

13 References and bibliography

This section lists all documentation used as source material for this report:

1. *Common Criteria for Information Technology Security Evaluation, Version 2.1*;

2. *CCS#4, Technical oversight, Canadian Common Criteria Evaluation and Certification Scheme (CCS), version 0.84 - Draft*;

3. *Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation methodology, Version 1.0*;

4. *Security Target Document Passport Certificate Server Ver. 4.1.1, Version 1.00*;

5. *Configuration Management System Passport Certificate Server V.4.1.1*;

6. *Passport Certificate Server Version 4.1.1 FUNCTIONAL SPECIFICATIONS for COMMON CRITERIA EVALUATION LEVEL: EAL2 (Augmented)*, 14 November, 2001;

7. *HIGH LEVEL DESIGN for COMMON CRITERIA EVALUATION EAL2 (augmented)*, 25 March 2002;

8. *DIVERSINET PASSPORT CERTIFICATE SERVER V 4.1.1 CORRESPONDENCE MAPPING*, 13 November 2001;

9. *INFORMAL SECURITY POLICY MODEL FOR DIVERSINET PASSPORT CERTIFICATE SERVER VERSION 4.1.1*, 4 March 2002;

10. *Delivery Procedure V2.0 Passport Certificate Server Version 4.1.1*;

11. *Passport Certificate Server Version 4.1.1 User's Guide*, June 2001;

12. *Security Functions Master Test Plan Passport Certificate Server V.4.1.1*;

13. *Evidence Of Developer Test Coverage Passport Certificate Server V.4.1.1*;

14. *ANALYSIS OF THE STRENGTH OF FUNCTIONALITY Of SECURITY MECHANISMS IN DIVERSINET PASSPORT CERTIFICATE SERVER v.4.1.1*;

15. *Vulnerability Analysis for Diversinet Passport Certificate Server version 4.1.1*, 29 November 2001;

16. Annex A of the *ETR*; and

17. Annex B of the *ETR*.

Supporting documentation:

18. *Passport Certificate Server: Cryptographic Protocols (Confidential)*; and

19. *Security Analysis and Commentary on the Diversinet SPEx Protocols*, 28 October 2000.