Certification Report

EAL 2 Evaluation of PGP Universal Server with Gateway and Key Management v2.9 running on Fedora Core 6

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-94
Version: 1.0
Date: 21 November 2008
Pagination: 1 to 9

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

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

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 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 that carried out this evaluation is the DOMUS IT Security Laboratory located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body 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.

This certification report is associated with the certificate of product evaluation dated 21 November 2008, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and http://www.commoncriteria.es

This certification report makes reference to the following trademarked or registered trademarks:

- PGP is a registered trademark and the PGP logo is a trademark of PGP Corporation
- Dell and Poweredge are trademarks of Dell Inc.
- IBM, BladeCenter, and System x are trademarks of International Business Machines Corporation in the United States, other countries, or both.
- HP, and HP ProLiant are trademarks of Hewlett-Packard Company
- Sun Fire is a trademark, registered trademark, or service mark of Sun Microsystems, Inc. in the U.S. and other countries.
- VMware is a registered trademark or trademark (the "Marks") of VMware, Inc. in the United States and/or other jurisdictions.

- Fedora is a trademark of Red Hat, Inc.
- NEC is a trademark and/or registered trademark of NEC Corporation in the United States and/or other countries.

TABLE OF CONTENTS

Executive Summary

PGP Universal Server with Gateway and Key Management v2.9 running on Fedora Core 6 (hereafter referred to as PGP Universal Server), from PGP Corporation®, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 evaluation.

PGP Universal Server is a proprietary software application designed to act as an email proxy. The purpose of the application is to provide encryption and signing services for email messages entering or leaving the local network. PGP Universal Server transparently encrypts or decrypts messages using a user's public key. If a user does not have a PGP key pair, PGP Universal Server automatically generates one for the user. PGP Universal Server manages a list of public keys for internal users and allows both internal and external users to access a list of public keys for internal users.

The DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 20 October 2008 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for PGP Universal Server, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in 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 EAL 2 assurance requirements for the evaluated security functionality. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2 (with applicable final interpretations), for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the PGP Universal Server evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation is PGP Universal Server with Gateway and Key Management v2.9 running on Fedora Core 6 (hereafter referred to as PGP Universal Server), from PGP Corporation®.

2 TOE Description

PGP Universal Server is a proprietary software application designed to act as an email proxy. The purpose of the application is to provide encryption and signing services for email messages entering or leaving the local network. PGP Universal Server transparently encrypts or decrypts messages using a user's public key. If a user does not have a PGP key pair, PGP Universal Server automatically generates one for the user. PGP Universal Server manages a list of public keys for internal users and allows both internal and external users to access a list of public keys for internal users.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for PGP Universal Server is identified in Section 6 of the Security Target (ST).

The following cryptographic module was evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
PGP Software Developer's Kit (SDK) Cryptographic Module v3.11.0	1049

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in PGP Universal Server:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	471
Advanced Encryption Standard (AES)	FIPS 197	453
Rivest Shamir Adleman (RSA)	ANSI x9.31	172
Secure Hash Algorithm (SHA-1)	FIPS 180-2	516
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	216
Digital Signature Algorithm (DSA)	FIPS 186-2	183
ANSI x9.31 RNG	ANSI x9.31	238

4 Security Target

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

Title: PGP Corporation® Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 Security Target
Version: 0.6
Date: 20 October 2008

5 Common Criteria Conformance

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2 (with applicable final interpretations), for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.

PGP Universal Server is:

a. Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2;
b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and
c. Common Criteria EAL 2 conformant, with all security the assurance requirements in the EAL 2 package.

6 Security Policy

PGP Universal Server implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies are found in Section 6 of the ST.

In addition, PGP Universal Server implements policies pertaining to security audit, cryptographic support, user data protection, identification and authentication, security management, protection of the TSF, and TOE access. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of PGP Universal Server should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the PGP Universal Server.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The TOE is installed and configured on the appropriate hardware according to the appropriate installation guides.
- There are one or more competent administrators assigned to manage the TOE and the security of the information it contains.
- The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
- The TOE and the hardware it runs on are physically available to authorized administrators only.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE environment provides the network connectivity required to allow the TOE to provide secure email proxy functions.
- All ports needed for proper operation of the TOE will be opened at the firewall.
- DNS information received by the TOE is reliable.
- Email messages cannot pass between the internal and external networks without passing through the TOE.
- The TOE shall be protected from external interference and tampering.

7.3 Clarification of Scope

PGP Universal Server was designed and intended for use in a structured corporate environment. In this type of environment, users will not typically be permitted to install programs on their machines or change system settings. Administrators will set policy that controls what users are, and are not, permitted to do.

Protection against attacks such as session hijacking[2] fall outside the PGP Universal Server intended use, and should be addressed by other security mechanisms such as firewalls and intrusion detection systems.

[2] Session hijacking refers to the exploitation of a valid computer session.

8 Architectural Information

PGP Universal Server is a proprietary software application designed to act as an email proxy and encryption gateway. PGP Universal Server comprises the subsystems:

- **Proxy Subsystem** that processes email traffic against the set of administer-created proxy rules and handles requests for users' keys;
- **Database, Preferences and Translation Subsystem** that manages PGP Universal Server data;
- **Web Subsystem** that provides web interfaces used to manage the PGP Universal Server;
- **Authentication and Ignition Subsystem** that authenticates users and handles the ignition process when the PGP Universal Server is configured to use an ignition key;
- **Audit and Operating System Subsystem** that relays requests between the PGP Universal Server and the underlying Fedora operating system; and
- **Cryptography Subsystem** that handles cryptographic operations for the PGP Universal Server.

Further details about the system architecture are proprietary to the developer, and are not provided in this report.

9 Evaluated Configuration

The PGP Universal Server evaluated configuration comprises PGP Universal Server with Gateway and Key Management v2.9 running on Fedora Core 6 installed on the following hardware platforms:

- Dell PowerEdge740
- Dell PowerEdge 860
- Dell PowerEdge 1950
- Dell PowerEdge 2950
- IBM System x346
- IBM System x3650
- IBM BladeCenter HS20 Type 7981
- Sunfire 4100
- HP Proliant BL25P
- NEC Express5800 120Ri-2
- VMWare ESX + VMtools 3.0.1
- HP Proliant DL 385 G2 w/ P400 RAID
- HP Proliant DL385 w/ P600 RAID

- HP Proliant DL385 w/ P800 RAID

10 Documentation

The PGP Universal Server documents provided to the consumer are as follows:

a. PGP Universal Server 2.9 Common Criteria Supplemental v1.2;

b. PGP Universal Server Administrator's Guide. PGP Universal Server Version 2.9.0. Released July 2008; and

c. PGP Universal Server Upgrade Guide. PGP Universal Server Version 2.9.0. Released July 2008.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of PGP Universal Server including the following areas:

Development: The evaluators analysed the PGP Universal Server functional specification and design documentation and determined that the design completely and accurately instantiated the security functional requirements. The evaluators analyzed the PGP Universal Server security architectural description and determined that the initialisation process was secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

Guidance Documents: The evaluators examined the PGP Universal Server preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the PGP Universal Server into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that it is complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the PGP Universal Server configuration management system and associated documentation was performed. The evaluators found that the PGP Universal Server configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of PGP Universal Server. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify PGP Universal Server potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the PGP Universal Server in its operational environment.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[3].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of DOMUS IT Security Laboratory test goals:

- Repeat of Developer's Tests: The objective of this test goal is to repeat the developer's tests;
- Audit: The objective of this test goal is to ensure that the System Event Logging and Access Logging requirements are met;
- Cryptographic Support: The objective of this test goal is to ensure that all cryptographic functionality is properly exercised;
- Identification and Authentication: The objective of this test goal is to ensure that access to the management capability is restricted to authorized administrators;
- User Data Protection: The objective of this test goal is to ensure that the role based access control policy is enforced;
- Security Management: The objective of this test goal is to ensure that authorized administrators are able to manage and configure the PGP Universal Server; and

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

- TOE Access: The objective of this test goal is to ensure that the PGP Universal Server terminates a user session after a period of 15 minutes of inactivity.

12.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Port Scanning;
- Monitoring the network traffic; and
- Denial-of-service.

The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment.

12.4 Conduct of Testing

The PGP Universal Server was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at DOMUS IT Security Laboratory. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the PGP Universal Server behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 2 level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

Consumers are advised to review the security aspects of the intended environment (defined in Section 3 of the ST) when deploying the PGP Universal Server.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description

Acronym/Abbreviation/ Initialization	Description
ANSI	American National Standards Institute
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
DNS	Domain Name System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
RNG	Random Number Generator
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

16 References

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

a. CCS Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

d. PGP Corporation® Universal Server with Gateway and Key Management v2.9 Running on Fedora Core 6 Security Target v0.6, October 20, 2008.

e. Evaluation Technical Report Version 1.4, PGP Corporation® Universal Server Gateway and Key Management v2.9 running on Fedora Core 6, EAL 2, October 20, 2008.