Certification Report

EAL 2 Evaluation of

Alacris OCSP Client Professional 4.0.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© 2004 Government of Canada, Communications Security Establishment

Evaluation number: 383-4-21
Version: 1.0
Date: January 13, 2004
Pagination: i to iii, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have 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 1.0*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1*. 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 (CSE), 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 CSE, 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.

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 CGI Information Systems and Management Consultants Inc., 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 13 January 2004, 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/en/services/common_criteria/trusted_products.html

This certification report makes reference to the following trademarked names: Alacris, which is a registered trademark of Alacris® Inc.; Windows NT and Windows 2000/2003/XP which are registered trademarks of Microsoft® Corporation.

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

TABLE OF CONTENTS

Executive Summary

The Alacris OCSP Client Professional 4.0.0, from Alacris® Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The Alacris OCSP Client Professional 4.0.0 provides an end user with the ability to query the revocation status of an X.509 public key certificate using the On-line Certificate Status Protocol (OCSP) documented in RFC 2560. The Alacris OCSP Client Professional 4.0.0 communicates with the Alacris OCSP Server, or any OCSP responder compliant with RFC 2560, to query the revocation status of certificates in the context of a Public Key Infrastructure (PKI).

CGI Information Systems and Management Consultants Inc. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 9 January 2004, 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 the Alacris OCSP Client Professional 4.0.0, 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 Alacris OCSP Client Professional 4.0.0 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[1] for this product indicate that it meets the EAL 2 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 1.0* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.1*.

The Communications Security Establishment, as the CCS Certification Body, declares that the Alacris OCSP Client Professional 4.0.0 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.

[1] The evaluation technical report 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 the Alacris OCSP Client Professional 4.0.0, from Alacris® Inc..

2 TOE Description

The Alacris OCSP Client Professional 4.0.0 provides an end user with the ability to query the revocation status of an X.509 public key certificate using the On-line Certificate Status Protocol (OCSP) documented in RFC 2560. The Alacris OCSP Client Professional 4.0.0 communicates with the Alacris OCSP Server, or any OCSP responder compliant with RFC 2560, to query the revocation status of certificates in the context of a Public Key Infrastructure (PKI).

See section 2 in the Security Target (ST) for a more complete, detailed description of the OCSP Client Professional.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Alacris OCSP Client Professional 4.0.0 is identified in Section 4.1 of the ST.

4 Security Target

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

Title: *Security Target for Alacris® OCSP Client Professional Version 4.0.0 (EAL2)*
Version: 1.0
Date: 9 January 2004

5 Common Criteria Conformance

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 Alacris OCSP Client Professional 4.0.0 is:

a) Common Criteria Part 2 extended, with a set of security functional requirements from Part 2 and additional security functional requirements as defined in section 4.1.1 of the ST;
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 the security assurance requirements in the EAL 2 package.

6 Security Policy

6.1 Confidentiality

The Alacris OCSP Client Professional 4.0.0 allows the configuration of an SSL session to protect the confidentiality of communications with OCSP responders.

6.2 Identification and Authentication

The Alacris OCSP Client Professional 4.0.0 allows a user to identify and authenticate themselves to an OCSP responder through the use of a digital signature as described in RFC 2560. The Alacris OCSP Client Professional 4.0.0 can identify and authenticate OCSP responses as coming from a valid OCSP responder through the use of digital signature verification, as described in RFC 2560.

6.3 Integrity

The Alacris OCSP Client Professional 4.0.0 uses digital signatures to verify the integrity of messages exchanged with OCSP responders. The use of nonces, as described in RFC 2560, is used to provide resistance to replay attacks.

6.4 Auditing

The Alacris OCSP Client Professional 4.0.0 generates security relevant audit events that are written to the OS audit repositories.

7 Assumptions and Clarification of Scope

Consumers of the Alacris OCSP Client Professional 4.0.0 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the Alacris OCSP Client Professional 4.0.0.

7.1 Secure Usage Assumptions

The following secure usage assumptions have been made, consistent with Section 2.3 in the ST:

a) SSL is configured for communication with OCSP responders;

b) The Alacris OCSP Client Professional 4.0.0 is configured to verify nonces in OCSP responses;
c) Signing of OCSP requests is enabled;
d) All logging and auditing is enabled; and
e) The Alacris OCSP Client Professional 4.0.0 is deployed on a supported operating system platform.

7.2 Environmental Assumptions

The following environmental assumptions, consistent with the ST, have been made during the evaluation of the Alacris OCSP Client Professional 4.0.0:

a) The host workstation for the TOE is assumed to be located within controlled access facilities that will prevent unauthorized physical access;
b) The host workstation for the TOE is assumed to be protected from unauthorized logical access using appropriate logical access controls;
c) Administrators and operators are neither careless nor willfully negligent and will abide by the instructions provided in the administrative guidance supplied with the TOE; and
d) The host workstation, software and associated devices function correctly and are maintained at regular intervals. Maintenance will include the application of standard security hardening techniques for the operating system platform, application of security patches and archiving of audit logs so as not to exceed storage limitations.

For more information about the TOE security environment, refer to Section 3 of the ST.

7.3 Clarification of Scope

As described in the ST and previous sections of this document, the Alacris OCSP Client Professional 4.0.0 is intended to be deployed in environments that provide a considerable amount of physical and logical security for the underlying operating system. As such, the Alacris OCSP Client Professional 4.0.0 does not counter any threats aimed at compromising the TSF or TSF Data through the subversion of the hosting operating system or the physical platform on which it resides.

Although the Alacris OCSP Client Professional 4.0.0 does make use of cryptography, it does not directly implement cryptographic algorithms or perform key generation. The cryptographic implementation used is that provided by the Windows® OS resident Cryptographic Application Programming Interface (CAPI) libraries, and was not in the scope of this evaluation.

8 Architectural Information

The major components comprising the TOE are:

a) The OCSP Client Service;
b) The Microsoft® Management Console (MMC) Snap-In; and
c) The Revocation Provider.

The OCSP Client Service component sends OCSP requests, validates OCSP responses, and provides logging functionality. The Microsoft® Management Console (MMC) snap-in component provides administrators an interface to the Alacris OCSP Client Professional 4.0.0 resource parameters stored in the Windows® registry. The MMC Snap-In is used to configure the Alacris OCSP Client Professional 4.0.0. The Revocation Provider integrates with the Microsoft Windows® CAPI to provide CAPI-enabled applications with on-line revocation checking capabilities.

9 Evaluated Configuration

The following OS platforms were used for the evaluation of the Alacris OCSP Client Professional 4.0.0:

a) Microsoft Windows® 2000 Professional with Service Pack 3 and High Encryption Pack for Windows® 2000;
b) Microsoft Windows® XP, Service Pack 1; and
c) Microsoft Windows® 2003 Enterprise Edition.

The following Alacris OCSP Client Professional 4.0.0 configuration was used for the evaluation:

a) SSL is configured for communication with OCSP responders;
b) The Alacris OCSP Client Professional 4.0.0 is configured to verify nonces in OCSP responses;
c) Signing of OCSP requests is enabled; and
d) All logging and auditing is enabled.

10 Documentation

The documentation for the Alacris OCSP Client Professional 4.0.0 consists of the online help distributed to the consumer in Microsoft® Help Format (accessible from within the TOE software) as well as the installation instructions, “readme” file and release notes in the root

directory of the CD that is delivered to the consumer. The filenames[2], as distributed on the CD containing the TOE, are:

- ocspclientv4.chm (user and administrator guidance);
- Alacris OCSP Client Installation Guide.mht;
- readme.txt; and
- ReleaseNotes.htm.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Alacris OCSP Client Professional 4.0.0, including the following areas:

Configuration management: An analysis of the Alacris OCSP Client Professional 4.0.0 development environment and associated documentation was performed. The evaluator found that the Alacris OCSP Client Professional 4.0.0 configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the OCSP Client Professional during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the Alacris OCSP Client Professional 4.0.0 functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the Alacris OCSP Client Professional 4.0.0 user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

[2] Individual version numbers are not provided for these documents as the documentation is packaged as a part of the product build. As such, the document version numbers are considered to be the same as the product version.

Vulnerability Assessment: The evaluators examined the developer's vulnerability analysis for the Alacris OCSP Client Professional 4.0.0 and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluator conducted an independent review of public domain vulnerability databases, relevant OCSP standards, and evaluation deliverables to provide assurance that all potential vulnerabilities have been considered.

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

12 ITS Product Testing

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

12.1 Assessing Developer Tests

The evaluators verified that the developer had met their testing responsibilities through an examination of the developer's test plans and procedures, a review of the test results, and an on-site visit to the developer's test facility. Additionally, the developer provided a coverage analysis, which the evaluators used to assess the correspondence between the developer's test plans and the functional specification for the TOE.

12.2 Independent Functional Testing

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

Independent execution of a large subset of the developer's tests was performed to gain assurance in the developer's testing effort. In order to gain assurance that the TOE Security Functions (TSF) operate in accordance with the functional specification on all developer recommended OS platforms, evaluators performed a subset of the developer's test procedures on each platform.

Independent evaluator tests were devised using the ST, functional specification, developer test evidence, and guidance documentation. The tests focused on:

- Installation and configuration;
- OCSP request generation;
- OCSP response verification; and

- Logging and auditing;

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis, independent evaluator penetration testing was deemed unnecessary, given the restrictive operating environment for the TOE, and the high level of sophistication and specialized tools that would be required to intercept and modify encrypted OCSP messages.

12.4 Conduct of Testing

The Alacris OCSP Client Professional 4.0.0 was subjected to a comprehensive suite of formally documented, independent functional tests. The testing took place at both the Alacris® Inc. facility in Ottawa, Ontario; and the ITSET facility at CGI Information Systems and Management Consultants Inc., located in Ottawa, Ontario. 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 the Evaluation Technical Report (ETR)[3].

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the Alacris OCSP Client Professional 4.0.0 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

As described in the ST and previous sections of this document, the Alacris OCSP Client Professional 4.0.0 is intended to be deployed in environments that provide a considerable amount of physical and logical security for the underlying operating system. As such, the Alacris OCSP Client Professional 4.0.0 does not counter any threats aimed at compromising the TSF or TSF Data through the subversion of the hosting operating system or the physical

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

platform on which it resides. Consumers are advised to review the ST and ensure that their deployment environment is consistent with the defined intended environment.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

Acronym/Abbreviation/Initialization	Description
CAPI	Cryptographic Application Programming Interface
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OCSP	Online Certificate Status Protocol
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
PKI	Public Key Infrastructure
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

16 References

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

a) Common Criteria for Information Technology Security Evaluation, CCIMB-99-031/032/033, Version 2.1, August 1999.

b) Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation and Methodology, Version 1.0, August 1999.

c) CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, 3 October 2002.

d) Security Target for Alacris® OCSP Client Professional Version 4.0.0 (EAL2), Version 1.0, 9 January 2004.

e) Evaluation Technical Report of the Alacris OCSP Client Version 4.0.0, Version 1.0, 12 December 2003.