Certification Report

EAL 2 Evaluation of Hitachi ID Management Suite Version 3.2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-37-CR
Version:	1.0
Date:	16 May 2008
Pagination:	i to iv, 1 to 11

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 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. This certification report, and its associated certificate, applies 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 DOMUS IT Security Laboratory, a division of NUVO Network Management, 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) to which the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 16 May 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.commoncriteriaportal.es.

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

- Hitachi ID Management Suite, P-Synch and ID-Synch are trademarks or registered trademarks of Hitachi ID Systems, Inc.

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

TABLE OF CONTENTS

Disclaimer i

Foreword ii

Executive Summary 1

1 Identification of Target of Evaluation 2

2 TOE Description 2

3 Evaluated Security Functionality 2

4 Security Target 2

5 Common Criteria Conformance 2

6 Security Policy 3

7 Assumptions and Clarification of Scope 3

7.1 SECURE USAGE ASSUMPTIONS 3
7.2 ENVIRONMENTAL ASSUMPTIONS 3
7.3 CLARIFICATION OF SCOPE 4

8 Architectural Information 4

9 Evaluated Configuration 4

10 Documentation 4

11 Evaluation Analysis Activities 5

12 ITS Product Testing 6

12.1 ASSESSMENT OF DEVELOPER TESTS 6
12.2 INDEPENDENT FUNCTIONAL TESTING 6
12.3 INDEPENDENT PENETRATION TESTING 7
12.4 CONDUCT OF TESTING 7
12.5 TESTING RESULTS 7

13 Results of the Evaluation 7

14 Evaluator Comments, Observations and Recommendations 7

15 Acronyms, Abbreviations and Initializations 8

16 References 8

Executive Summary

The Hitachi ID Management Suite Version 3.2, (hereafter referred to as the ID Management Suite), from Hitachi ID Systems, Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The ID Management Suite is a complete identity and password management software solution enabling organizations to securely organize and manage user identities across enterprise applications and systems.

DOMUS IT Security Laboratory, a division of NUVO Network Management, is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 25 April 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 the ID Management Suite, 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 IT Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.3*.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Hitachi ID Management Suite Version 3.2 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 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 Hitachi ID Management Suite Version 3.2, (hereafter referred to as the ID Management Suite), from Hitachi ID Systems, Inc.

2 TOE Description

ID Management Suite is an identity and password management software solution enabling organizations to securely organize and manage user identities across enterprise applications and systems. ID Management Suite comprises the components ID-Synch that provides identity management across multiple platforms, both current and legacy, and P-Synch that provides a uniform password management policy across an enterprise. Additional detail on ID-Synch and P-Synch can be found in Section 2 of the ST.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for ID Management Suite is identified in Section 6 of the ST.

4 Security Target

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

Title: Hitachi ID Management Suite Version 3.2 Security Target (EAL2)
Version: Version 1.98
Date: 21 April 2008

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.3.*

The ID Management Suite is:

a) Common Criteria Part 2 extended, with security functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST: FAU_ADG.1;

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, containing all security assurance requirements in the EAL 2 package.

6 Security Policy

ID Management Suite implements the discretionary access control policies ID-Synch Protected User Record Access Control and P-Synch Protected User Record Access Control; details of these security policies can be found in Sections 5 of the ST.

In addition, ID Management Suite implements policies pertaining to security audit, user data protection, identification and authentication, security management, and protection of the TOE security functions. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of ID Management Suite 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 ID Management Suite.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- System administrators are competent to manage the TOE and the security of the information it contains. The administrators will not compromise the security of the TOE or its data either willfully or by neglect.

- Users cooperate with those responsible for managing the TOE to maintain TOE security and will follow all directives and prescriptions imposed by the administrators and / or guidance provided with the TOE.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The environment is secure and the administrators have a good working knowledge and know how to manage the OS underlying the TOE.

- The network connected to the TOE is protected from active attacks (i.e. data mode intrusion).

7.3 Clarification of Scope

ID Management Suite was designed and intended for use in a structured corporate environment. It can not prevent authorized administrators from carelessly configuring the TOE such that the access control policies are compromised.

ID Management Suite provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone.

While the ID Management Suite user guidance documents do provide adequate advice for securing its operational environment, it is primarily the users' responsibility in ensuring that the networks and the systems which ID Management Suite is connected to or installed on, are adequately protected.

8 Architectural Information

ID Management Suite comprises the main components ID-Synch that provides identity management; P-Synch that provides password management; and P-Synch/390 which is a proprietary started task and security exit agent installed on the IBM OS/390 operating system. Section 2 of the ST identifies ID Management Suite subsystems (Self-service, Consolidated administration, Service infrastructure, and OS/390 local agent); Figure 3 in the ST provides a pictorial description of the subsystems relationships. Further details about the system architecture are proprietary to the vendor, and are not provided in this report.

9 Evaluated Configuration

The evaluated configuration comprises:

- ID-Synch revision 3.2.0, build 0.1279, running on Windows 2003 Server SP2;
- P-Synch revision 6.2.9, build 2.3407, running on Windows 2003 Server SP2 ; and
- OS390 Agent build 2.1.0, running on OS/390.

10 Documentation

The user documentation for the ID Management Suite consists of the following:

- Locking Down an ID Management Suite Server, Software revision: 3.2.0, Hitachi ID Management Suite revision: 3.2.0, Last changed: April 21, 2008.

- ID-Synch Installation and Configuration Guide, ID-Synch Software revision: 3.2.0, Hitachi ID Management Suite revision: 3.2.0, Last changed: April 21, 2008.

- P-Synch Installation and Configuration Guide, P-Synch Software revision: 6.2, Hitachi ID Management Suite revision: 3.2.0, Last changed: April 21, 2008.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of ID Management Suite, including the following areas:

Configuration management: An analysis of the ID Management Suite configuration management system and associated documentation was performed. The evaluators found that the ID Management Suite 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.

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 ID Management Suite 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 ID Management Suite 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 ID Management Suite administrator and user guidance documentation and determined that it sufficiently and unambiguously described how to securely administer and use the product, and that it was consistent with the other documents supplied for evaluation.

Vulnerability assessment: The ID Management Suite ST’s strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer’s vulnerability analysis for the ID Management Suite 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 evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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

12 ITS Product Testing

Testing at EAL2 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 [2].

The evaluators analyzed the developer's test coverage analysis and found it to be accurate.

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 test goals:

The tests focused on the following areas, based upon the security functional requirements in the ST and the security functions defined in the functional specification:

- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;
- Audit: The objective of this test goal is to ensure that audit requirements have been met;
- Identification and Authentication: The objective of this test goal is to ensure that access to the ID Management Suite was restricted to authorized personnel only;
- Discretionary access control: The objective of this test goal is to ensure that the security policy rules are enforced;
- Security Management: The objective of this test goal is to ensure that authorized administrators are able to manage and configure the ID Management Suite; and

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

- Secure Transfer: The objective of this test goal is to ensure that confidentiality of the data transmitted between different parts of the TOE is protected.

12.3 Independent Penetration Testing

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

- Common web application vulnerabilities;
- Port Scanning; and
- Network traffic-based attack.

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

12.4 Conduct of Testing

The ID Management Suite was subjected to a comprehensive suite of formally-documented, independent functional and penetration tests. The testing took place at the developer’s site located in Calgary, Alberta, Canada*,* and at the ITSET facility at DOMUS IT Security Laboratory located in Ottawa, Ontario, Canada. 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 separate Test Results document.

12.5 Testing Results

The developer’s tests and independent functional tests yielded the expected results, giving assurance that the ID Management Suite 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

ID Management Suite includes comprehensive guidance documents for the installation, configuration and operation of the product.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CR	Certification Report
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
ST	Security Target
TOE	Target of Evaluation

16 References

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

a) Canadian Common Criteria Evaluation and Certification Scheme (CCS) Publication #4, Technical Oversight, Version 1.0.

b) Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

c) Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3, August 2005.

d) Hitachi ID Management Suite Version 3.2 Security Target (EAL2), Version 1.98, 21 April 2008.

e) Evaluation Technical Report for EAL2 Evaluation of Hitachi ID Management Suite Version 3.2, Version 1.2, 25 April 2008.