Certification Report

EAL 3 Evaluation of InterSystems Corporation

InterSystems Caché 5.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-32-CR
Version: 1.0
Date: 15 February 2007
Pagination: i to iv, 1 to 9

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 2.2*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.2*. 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 (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 (CSE).

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 Electronic Warfare Associates-Canada, Ltd. 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 15 February 2007, 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 and on the official Common Criteria Program website at http://www.commoncriteriaportal.org

This certification report makes reference to the trademarked name: Caché which is a registered trademark of the InterSystems Corporation.

TABLE OF CONTENTS

Executive Summary

The InterSystems Caché 5.1, from InterSystems Corporation, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation.

The InterSystems Caché 5.1 is a post-relational database software program that offers three integrated data access options which can be used simultaneously on the same data: a robust object database, high performance *Structured Query Language* (SQL), and rich multidimensional access. No mapping is required between object, relational, and multidimensional views of data, resulting in savings in both development and processing time. Caché enables rapid Web application development, rapid transaction processing speed, massive scalability, and real-time queries against transactional data.

EWA-Canada is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 14 February 2007, 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 InterSystems Caché 5.1, the security requirements, and the level of confidence (evaluation assurance level) to which the product is intended to satisfy the security requirements. Consumers of the InterSystems Caché 5.1 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 (ETR)[1] for this product provide sufficient evidence that it meets the EAL 3 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.2 r326* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.2 r326*.

The Communications Security Establishment, as the CCS Certification Body, declares that the InterSystems Caché 5.1 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) at http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official International Common Criteria Program website at http://www.commoncriteriaportal.org.

.

[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) 3 evaluation is the InterSystems Caché 5.1, from InterSystems Corporation.

2 TOE Description

The TOE is a post-relational database software program that offers three integrated data access options which can be used simultaneously on the same data: a robust object database, high performance *Structured Query Language* (SQL), and rich multidimensional access. No mapping is required between object, relational, and multidimensional views of data, resulting in savings in both development and processing time. Caché enables rapid Web application development, rapid transaction processing speed, massive scalability, and real-time queries against transactional data.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the InterSystems Caché 5.1 is identified in Section 5 of the ST.

4 Security Target

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

Title: InterSystems Corporation Caché v5.1.0.826.0, Security Target
Version: 1.1
Date: 02 January 2007

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.2 r326*, for conformance to the *Common Criteria for IT Security Evaluation, version 2.2 r326*, incorporating all applicable final CC interpretations. The InterSystems Caché 5.1 is:

a) Common Criteria Part 2 conformant, with security functional requirements based upon functional components in Part 2 as well as the following explicitly defined security functional requirements:
   - FAU_STG.NIAP-0414 – Site-Configurable Prevention of Audit Loss; and
   - FPT_ITD_EXP.1 – SFP Domain Separation;

b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c) Common Criteria EAL 3 conformant with all the security assurance requirements in the EAL 3 package.

6 Security Policy

The InterSystems Caché 5.1 implements a Discretionary Access Control security functional policy. This policy implements a typical discretionary access control model where each object in the database has an owner who may assign access permissions on the object to other database users or groups of users. The TOE enforces the policy on all operations by all database users on all database objects.

The InterSystems Caché 5.1 implements policies pertaining to audit, identification and authentication, management of security attributes, and protection of the TOE security functions. InterSystems Caché 5.1 policy detail can be found in Section 5.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the InterSystems Caché 5.1 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 product.

7.1 Secure Usage Assumptions

Administrators who are entrusted to install, configure and maintain the TOE are non-hostile, appropriately trained and follow all appropriate guidance instructions.

There are no general purpose computing capabilities such as compilers or other applications installed on server platforms on which the TOE is installed, except where such capabilities are necessary to support the operation of the TOE.

7.2 Environmental Assumptions

The environment in which the TOE resides provides physical protection for the TOE (for example against theft or vandalism) which is commensurate with the value of the resources stored within the TOE.

The operating system upon which the TOE is installed provides a robust computing environment and that secure data communications are available for use by the TOE in the transmission of TOE data.

7.3 Clarification of Scope

The InterSystems Caché 5.1 is a software product. The TOE relies upon the underlying operating system for the following security functional requirements:

- FPT_RVM.1 – Non-bypassibility (in conjunction with the TOE);
- FPT_SEP.1 – Domain separation; and
- FPT_STM.1 – Reliable Time Stamps.

8 Architectural Information

The InterSystems Caché 5.1 is a software product which implements a database system incorporating multiple access methods. The underlying hardware and operating systems on which the TOE functions provide permanent storage for the database objects as well as shared memory resources which are utilized by the TOE. The TOE's design incorporates subsystems which perform the following major functions:

- Provide user authentication services (the TOE supports a number of authentication mechanisms including proxied and client/server Kerberos authentication and local username/password authentication);
- Interpret and compile user requests for operations on database objects; and
- Interface with the operating system for the storage, retrieval and manipulation of database objects.

9 Evaluated Configuration

The InterSystems Caché 5.1 is a software product which runs on top of a number of different operating systems. For the purposes of the evaluation, the evaluated configuration of the TOE consisted of Version 5.1.0.826.0 of the TOE on the following operating systems:

- Windows Server 2003;
- Red Hat Enterprise Linux AS (Intel 32 bit) Version 4; and
- OpenVMS for Alpha Version 8.2.

10 Documentation

The InterSystems Caché 5.1 documents provided to the consumer are as follows:

- InterSystems Caché, Caché System Administration Guide, Version 5.1, 15 June 2006;
- InterSystems Caché, Caché Security Administration Guide, Version 5.1, 15 June 2006;
- InterSystems Caché, Caché Installation Guide, Version 5.1, 15 June 2006;
- InterSystems Corporation, Caché 5.1.0.826.0, ADM Readme, Document Version 0.3, 2 January 2007;
- InterSystems Corporation, Caché 5.1.0.826.0, IGS Readme, Document Version 0.4, 2 January 2007;

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the InterSystems Caché 5.1, including the following areas:

Configuration management: An analysis of the InterSystems Caché 5.1 development environment and associated documentation was performed. The evaluators found that the InterSystems Caché 5.1 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 InterSystems Caché 5.1 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 InterSystems Caché 5.1 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 InterSystems Caché 5.1 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.

Life-cycle support: The evaluators assessed the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the InterSystems Caché 5.1 design and implementation.

Vulnerability assessment: The strength of function claims in the ST were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the InterSystems Caché 5.1 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. Penetration testing was conducted by evaluators, which did not expose any residual vulnerabilities that would be exploitable in the intended operating environment for the TOE.

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

12 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing the developer's test in terms of coverage and depth, performing independent functional tests, and performing independent penetration tests.

12.1 Assessing Developer Tests

The evaluator assessed InterSystem's test documentation for both coverage and depth. InterSystem's testing effort included multiple tests for each of the security functions provided by the product. InterSystem's testing effort also exercised all of the security relevant functionality of each of the externally visible TOE interfaces.

In selecting a subset of the developer's tests for repetition during the evaluation, the evaluators selected a sample of approximately 30% of the developer's tests. Tests were selected across the entire range of product security functionality and included at least one test procedure for each of the security functions claimed by the TOE.

12.2 Independent Functional Testing

In order to develop independent functional tests, the evaluators examined the design and guidance documentation as well as the security target and the developer's test documentation. The developer's test documentation covered all security functions and subsystems of the TOE in considerable detail leaving no obvious candidates for additional independent testing. However, by considering the critical security functions of the TOE, the evaluators decided to focus the independent functional testing on the following areas:

- Audit and audit reporting;
- Identification and authentication; and
- Users and roles (Discretionary Access Control security functional policy).

All testing was planned and documented to a sufficient level of detail to allow repeatability of the test procedures and results. All independent functional tests yielded the expected results.

12.3 Independent Penetration Testing

The developer's vulnerability analysis did not reveal any potential vulnerabilities of the TOE. This result was confirmed by an independent vulnerability analysis performed by the evaluators. Since this vulnerability analysis did not yield any potential areas of attack, the evaluators resorted to general attack methods employed against other database products. The areas listed below were selected as possible exploitable weaknesses in the TOE.

The penetration tests focused on:

- Deliberate misuse of installation instructions;
- Bypass attempts;
- Direct attacks on underlying data storage; and
- Attempts to bypass discretionary access controls.

No exploitable vulnerabilities were uncovered during the independent penetration testing.

12.4 Conduct of Testing

The InterSystems Caché 5.1 was subjected to a comprehensive suite of formally-documented, independent, functional and penetration tests. The testing took place at the InterSystems Corporation's facility in Cambridge MA, and the Information Technology Security Evaluation and Test (ITSET) facility at Electronic Warfare Associates-Canada, Ltd 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)[2].

12.5 Testing Results

The developer's test and independent functional tests yielded the expected results, giving assurance that the InterSystems Caché 5.1 behaves as specified in its ST and functional specification. The penetration testing resulted in a PASS verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in the InterSystems Caché 5.1 in its intended operating environment.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 3 level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

[2] 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.

14 Evaluator Comments, Observations and Recommendations

Over the course of the evaluation the evaluators noted that the TOE is a mature product supported by a well established development team which has an exceptionally strong focus on customer service. The evaluators also observed that TOE documentation is complete, accurate and highly professional in presentation.

15 Glossary

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

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
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
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) Common Criteria for Information Technology Security Evaluation, CCIMB-2004-01-001/002/003, Version 2.2 r326, December 2004.

b) Common Methodology for Information Technology Security Evaluation, CCIMB-2004-01-004, Part 2: Evaluation and Methodology, Version 2.2 r326, December 2004.

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

d) InterSystems Corporation Caché 5.1.0.826.0, Security Target, Document Version 1.1, 2 January 2007.

e) Evaluation Work Plan, Document Number 1488-000-D001, Version 1.2, 24 April 2006.

f) Common Criteria Evaluation Site Visit Report, InterSystems Corporation Caché 5.1, EAL 3 Evaluation, Document Number 1488-000-D006, V1.1, 11 May 2005.

g) Evaluation Test Plan for InterSystems Corporation Caché 5.1, Document Number 1488-000-D003, V1.0, 22 November 2006.

h) Evaluation Test Procedures for InterSystems Corporation Caché 5.1, Document Number 1488-000-D004, V1.0, 22 November 2006.

i) Evaluation Test Results for InterSystems Corporation Caché 5.1, Document Number 1488-000-D005, V1.0, 3 January 2007.

j) Evaluation Technical Report for EAL 3 Evaluation of InterSystems Caché 5.1, Document Number 1488-000-D002, Version 1.1, 14 February 2007.