National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

IBM® DB2® Content Manager Enterprise Edition V8.4 FP1A

Report Number: CCEVS-VR-VID10220-2009
Dated: 27 January 2009
Version: 2.1

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Kenneth Eggers

Common Criteria Testing Laboratory

Terrie Diaz, Lead Evaluator
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the IBM® DB2® Content Manager Enterprise Edition V8.4 FP1A.

The Validation Report presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of IBM® DB2® Content Manager Enterprise Edition V8.4 FP1A was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on 10 November 2008.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 extended and Part 3 conformant, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2. The product is not conformant with any published Protection Profiles. All security functional requirements are derived from Part 2 of the Common Criteria or expressed in the form of Common Criteria Part 2 requirements.

The TOE is IBM® DB2® Content Manager Enterprise Edition V8.4 FP1A. IBM® DB2® Content Manager Enterprise Edition is a data management system (content management system) that provides a foundation for managing, accessing, and integrating critical business information on demand.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

During this validation, the Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products, desiring a security evaluation, contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1a
Protection Profile	Not applicable
ST	IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1a Security Target, Version 1.0, 22 December 2008
Evaluation Technical Report	Evaluation Technical Report For IBM® DB2® Content Manager Enterprise Edition V8.4 FP1A (Non-Proprietary), Version 2.0 18 November 2008, Part 2

Item	Identifier
	(Proprietary), Version 2.0 19 November 2008
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005
Conformance Result	CC Part 2 extended and Part 3 conformant, EAL 4 augmented with ALC_FLR.2
Sponsor	International Business Machines (IBM)
Developer	International Business Machines (IBM)
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Evaluation Personnel	Science Applications International Corporation: Terrie Diaz, Dawn Campbell
Validation Body	NIAP CCEVS: Paul Bicknell, Kenneth Eggers

3 Organizational Security Policy

This section summarizes the security functions provided by IBM Content Manager that are evident at the various identified network interfaces. It is based on information provided in the Security Target.

3.1 Security audit

The TOE can audit system administration and item events.

System administration events comprise actions performed by an administrator in the System Administration Client or in a custom application. These events include defining users, assigning privileges, assigning access control lists to an object, and user logins. The administrator has the capability to enable or disable auditing of system administration events by modifying the Library Server configuration.

Item events are actions performed against specific objects within a Resource Manager or the object's indexing information within the Library Server. The administrator enables or disables auditing of item events by modifying an item's item type. The administrator can specify, for each item type defined in the TOE, any combination of the following actions to be audited: create; retrieve; update; and delete.

Each event log entry contains the following information: date and time the event occurred (obtained from the IT environment); event code (event type); item type (resource type); identity of the subject that performed the action that triggered the generation of the entry

(user name); and for item events the item ID of the object acted upon. The type of event log generated and the contents of the log define the outcome of the action.

The Library Server logs the events into event tables stored on and protected by the Library Server database located in the IT Environment. The database prevents any modification or deletions to the event tables that were not authorized by an authorized administrator.

3.2 Identification and authentication

The non-administrative users of the TOE are defined in the TOE and access the TOE via the Client for Windows or a WAS application. When a non-administrative user attempts to access the TOE, the user is identified and authenticated against the user's information stored in the user definition table of the Library Server.

The administrative users of the TOE are defined in the IT environment and access the TOE via the System Administration Client. The administrative user's user name must also be defined in the Library Server with full Content Manager administrative privileges. When an administrative user attempts to access the TOE, the TOE passes the information to the IT environment to identify and authenticate the user and upon successful authentication by the IT environment, the user is then identified against the user name stored in the Library Server. The user name in the Library Server must match the user name of the underlying operating system. Once the users are successfully identified and authenticated, access to the TOE and its resources is granted.

When a user logs on to the TOE, the TOE generates a User Token that represents the session under which the user can perform operations. The User Token is generated from information including the user name and the date and time the user logged on. When the user logs on, both the logon information and the User Token are returned to the API. The logon information and the User Token are then included in subsequent requests from the API to the Library Server. The Library Server can then identify the session under which the operation is being requested.

Each user account includes a counter that tracks the number of unsuccessful attempts to authenticate into the Contact Manager. This counter is reset upon successful authentication. When the administrator-configured number of allowed attempts is exceeded, the TOE locks the user account until the authorized administrator unlocks the account by resetting the counter to zero.

3.3 User data protection

Access to the TOE's resources is governed by the resource's Access Control List (ACL) that identifies the user and the access allowed. The TOE uses privileges to define what operations a user is allowed to perform on the resources. The Library Server verifies that the user has the required privilege and the ACL associated to the requested object grants access. The process the TOE implements to determine if access is granted is as follows:

- If administrative domains have been enabled, the resource must either be in the PUBLIC domain or be in the same domain as the user in order for the user to be able to request an operation on the resource; and

- The user must have the appropriate privilege to perform the requested operation. If the user does not have the appropriate privilege, the user is unable to perform the requested operation on any resource; and
- The user must have appropriate authorization to access the resource with the requested operation:
    - If the user possesses the ItemSuperAccess privilege, then ACL checks are bypassed. Otherwise, the TOE then identifies the applicable binding level, which determines the ACL that will be used in the access control decision. The binding level can be Item or Item Type.
    - The ACL defines what operations the user is authorized to perform on the controlled resource. Authorization can be granted via one of three rule types, which are processed in the following order of precedence:
        - Public—authorizes the ICMPUBLC user group (i.e., all users). The performance of this check is controlled by a library server configuration parameter and is disabled by default;
        - User—authorizes identified users; and
        - Group—authorizes a user group.

The TOE determines if the ACL authorizes the user to perform the requested operation, based on the ACL rules assigning authorizations to perform specific operations to the public, specific users, and/or specific groups.

A privilege is the right to perform an action in the TOE. Privileges are classified as either administration privileges or data access privileges. Administration privileges grant rights to model user data and administer the TOE, while data access privileges grant rights to perform operations on controlled resources.

Each user is assigned a set of privileges that defines the actions the user is allowed to perform in the TOE, including operations on controlled resources (though the ACL on a controlled resource still needs to authorize the user to perform a requested action on that resource).

If the TOE (specifically, the Library Server) grants an access request, the TOE generates an Object Token and returns this to the client making the access request via the API. The Object Token is also sent to the Resource Manager responsible for the requested item. The Object Token includes the identification of the item to which access is granted, the identity of the user to whom access has been granted, the operations that have been granted, and an expiration time. The client that has successfully requested access from the Library Server submits the Object Token and the necessary access request information via a URL to the Resource Manager, which then verifies the Object Token and access request information against the Object Token received from the Library Server. In this way, the Resource Manager can determine that the access request has been granted by the Library Server and has not expired, and can return the requested item to the requesting client.

3.4 Security management

The System Administration Client provides the interface utilized by the authorized administrator to perform the administrative functions. These functions include:

- The ability to select if administrative events and which type of item events will be logged in the event tables. This capability is restricted to the authorized administrator.
- The ability to modify the behavior of the access control function by enabling or disabling Public Access, which determines whether or not the access control function checks for authorizations granted to the ICMPUBLC group. This capability is restricted to the authorized administrator.
- The ability to modify the unsuccessful login attempts threshold. This capability is restricted to the authorized administrator.
- The ability to unlock the user accounts. This capability is restricted to the authorized administrator.
- The ability to specify: the ACLs to be assigned to protected resources and as user defaults, which is restricted to the authorized administrator; and the ability to specify an alternative ACL associated to a resource when the resource is created, which is restricted to the authorized administrator and the authorized non-administrative user assigned the 'ItemSetSysAttr', 'ItemSetACL' or 'UserACLOwner' privilege.
- The ability to create, modify, and delete administrative ACLs. This capability is restricted to the authorized administrator.
- The ability to create, modify, and delete user ACLs. This capability is restricted to the authorized administrator and the authorized non-administrative user assigned the 'UserACLOwner' privilege.
- The ability, when administrative domains are enabled, to modify the domain that users, groups, privilege sets, ACLs, resource managers and collections belongs to. This capability is restricted to the authorized administrator.
- The ability to create, query, modify, and delete the following user security attributes: user name, group membership, privileges, domain. This capability is restricted to the authorized administrator.
- The ability to modify which ACL is associated with a resource. This capability is restricted to the authorized administrator and the authorized non-administrative user assigned the 'ItemSetSysAttr', 'ItemSetACL' or 'UserACLOwner' privilege.
- The ability to modify the password for any user defined in Content Manager. This capability is restricted to the authorized administrator.

3.5 Protection of the TSF

Access to the administrative functions by the administrator and to resources by users is only possible if the user and administrator are successfully identified and authenticated.

The TOE uses the identification and authentication mechanism and the privileges associated to the users to ensure a secure domain for the user within the TOE at its interfaces. The identification and authentication mechanism ensures that TOE interfaces are isolated to the identified user and the privileges determines what rights that user has on the TOE and what actions the user will be able to perform within the TOE. The IT environment provides the secure operating system for a real-time domain where the TOE software executes which ensures that the TOE will not be bypassed or tampered with.

4 Assumptions and Policies

The statement of TOE security environment describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be deployed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product and the organizational security policies which the product is designed to comply.

Following are the assumptions identified in the Security Target:

- It is assumed the TOE will be located within controlled facilities which will prevent unauthorized physical access and modification.
- It is assumed Authorized users of the TOE will keep all their authentication data private.
- It is assumed one or more competent individuals are assigned to manage the TOE and the security of the information it contains.
- It is assumed those responsible to manage the TOE are competent individuals, that only authorized users can gain access to the TOE, and that they are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
- It is assumed that the operating systems have been configured in accordance with the manufacturer's installation guides and where applicable, in its evaluated configuration. It is securely configured such that the operating systems protect the TOE from any unauthorized users or processes.
- It is assumed the underlying operating environment will provide protection to the TOE and its stored, processed, and transmitted data, and a reliable system time.

Following are the organizational security policies levied against the TOE and its environment as identified in the Security Target.

- The TOE must limit the access to, modification of, and destruction of the resource objects to those users that are authorized to access the resource object.
- Users of the system shall be held accountable for their security relevant actions within the system.
- Only those users who have been authorized to access the information within the TOE may access the TOE.

- The TOE must provide authorized administrators with utilities to effectively manage the security-related functions of the system.
- The TOE must maintain a domain for its own execution that protects itself and its resources from external interference, tampering or unauthorized disclosure, through its own interfaces.

5 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made; and meets them with only a certain level of assurance (EAL 4 augmented in this case).
- Content Manager is a data management system (content management system) that provides a foundation for managing, accessing, and integrating critical business information on demand. Content Manager is able to integrate many forms of data — document, Web, image, rich media — across diverse business processes and applications, including Siebel, PeopleSoft, and SAP, presenting the data in an integrated context for later use.
- The TOE uses special-purpose, and evaluated, APIs (i.e., Content Manager 8.4 Connector APIs) to communicate between its various components. However custom developed applications, built using APIs, are considered to be outside of the evaluated configuration. The use of any TOE interfaces, other than those provided by the various Client components (i.e., Windows Client, the System Administration Client, or the WAS) are also considered to be outside of the evaluated configuration.
- Encryption of passwords with the ICC ToolKit, is performed in the IT environment, and the ST includes IT Environment Security Functional Requirements. Cryptographic protection of communications between TOE components is not provided, however a security objective on the IT Environment requires that the "communications between the TOE components be protected. This places the entire responsibility for protecting TOE communications on the buyers and necessitates careful network design and configurations.

6 Architectural Information[1]

The components of Content Manager comprise: a Library Server; one or more Resource Managers, the Content Manager 8.4 Connector Application Programming Interfaces (APIs); the System Administration Client; and the Client for Windows.

[1] Extracted from SAIC Final ETR Part 1 Version 2.0, 18 November 2008

The Library Server is the key component of the Content Manager system. The Library Server resides on a DB2 Enterprise Server database environment. It is called the Library Server because it performs the functions that a library catalog file in a real library performs. The Library Server manages the content metadata and is responsible for identification and authentication for non-administrative users and identification for administrative users requesting services from Content Manager and access control to the resources residing on Resource Managers. The Library Server manages the relationships between items in the system and controls access to all of the system information, including the information stored in the Resource Managers. The Library Server processes requests (such as update or delete) from one or more clients. In Content Manager, all access to the Library Server is via stored procedures. The Library Server code is co-resident with the database engine code. The Library Server passes back to the client query results that include object tokens and locators for requested content that the user is authorized to access. The database is not part of the TOE.

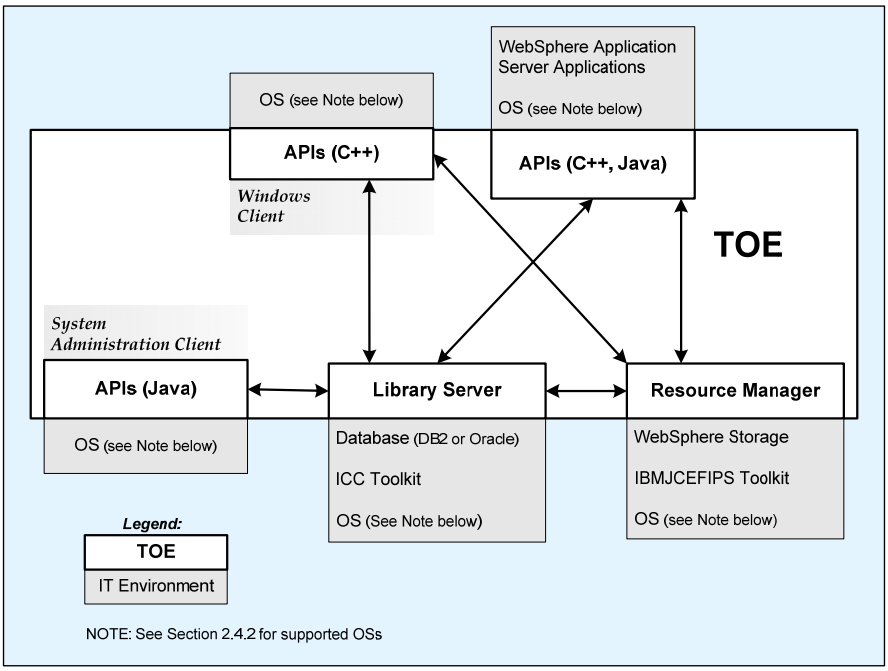
The Resource Manager stores resources for Content Manager. It can be on the same server as the Library Server, or it can be on its own computer. Resource Managers can be distributed across networks to provide convenient user access. Users store and retrieve digital resources on the Resource Manager by routing requests through the Library Server. A single Library Server can support multiple Resource Managers and content can be stored on any of these Resource Managers. When the Library Server grants an access request, the Library Server returns an object token and the location of the object to the user. Data objects are always associated with a specific collection on a Resource Manager. Access decisions to grant access to a collection of data objects are made by the Library Server and enforced by the Resource Manager. The client communicates directly with the Resource Manager using Internet protocols. Tokens received from the Library Server are passed to Resource Managers from a client through the APIs to provide assurance that the request has been authorized and the access control information has not been altered since leaving the Library Server. The Resource Manager requires the following components in the IT environment (both of which are provided in the Content Manager installation package as a convenience to users):

- DB2 Enterprise Server database—required to run the Resource Manager database, which stores information pertaining to the objects being managed by the Resource Manager
- WebSphere Application Server—required to run the Resource Manager, which is implemented as a Java2 Enterprise Edition (J2EE) web application.

The Content Manager 8.4 Connector APIs (used by WebSphere Application Server applications, the System Administration Client, and Client for Windows) comprise a set of object-oriented APIs that allow applications and users to access the Library Server and Resource Manager(s) and are used to facilitate all functions within the TOE, including administrative functions. Note that these APIs are identified in the three boxes labeled ‘APIs’ in the figure below.

The System Administration Client oversees the entire Content Manager system. From the System Administration Client, an administrator performs various administrative functions, such as defining the data model, creating users and defining their access to the system and

specific objects, and managing storage and storage objects in the system. The System Administration Client can be installed on any workstation with the other components or on its own workstation. The Client for Windows provides an interface that enables an application to import documents into Content Manager, view them, work with them, store them, and retrieve them. Note that the System Administration Client and Client for Windows are both part of the TOE and serve to facilitate human access to their underlying programmatic APIs.



The communication between the TOE components: Client for Windows, System Administration Client, Library Server, Resource Manager and the set of APIs should be protected as deemed necessary. The ST assumes that the channels would be protected to the degree necessary by available external means (e.g., physical network protection or some VPN technology).

7 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

Design documentation

Document	Version	Date
IBM DB2 Content Manager for Enterprise Edition Version 8.4 Fix Pack 1A Security High-level Functional Specification And Design	Issue 0.16	19 November, 2008
IBM DB2 Content Manager Enterprise Edition Version 8.4	Issue 0.11	19 November

Document	Version	Date
Fix Pack 1A Low-level Design Specification		2008
CM 84_DesignDocMapping_V.9.xls		
IBM® DB2® Content Manager Enterprise Edition Version 8.4 FP1A Informal Security Policy Model	Version 0.1	9 June 2008

Guidance documentation

Document	Version	Date
DB2 Content Manager Enterprise Edition, DB2 Content Manager for z/OS System Administration Guide Version 8 Release 4	SC27, SC27-1335-09	
System administration online help is available at http://publib.boulder.ibm.com/infocenter/cmgmt/v8r4m0/index.jsp		
DB2 Content Manager Enterprise Edition, DB2 Content Manager for z/OS Messages and Codes Version 8 Release 4	SC27-1349-07	
ICMClientHelpENU.zip		
DB2 Content Manager Enterprise Edition DB2, Content Manager for z/OS Application Programming Guide Version 8 Release 4	SC27-1347-08	
[API-REF] http://publib.boulder.ibm.com/infocenter/cmgmt/v8r4m0/index.jsp?topic=/com.ibm.cmgmttoc.doc/apihelp.htm		

Configuration Management documentation

Document	Version	Date
IBM DB2 Content Manager Enterprise Edition v8.4 Configuration Management	Issue 0.9	5 November 2008
IBM DB2 Content Manager Submitted documentation list		5 September 2008

Delivery and Operation documentation

Document	Version	Date
IBM DB2 Content Manager Enterprise Edition V8.4, Delivery, Operation and Guidance	Issue 0.5	24 June 2008
IBM DB2 Content Manager Enterprise Edition Version 8 Release 4 Planning and Installing Your Content Management System	GC27-1332-07	
DSW Secure Media Delivery (SMD)	v1.2	
Download Director Command Line Client (DDP) User Guide	Version 3.01	Aug 16, 2004

Document	Version	Date
Tequila for eSD and Golden Master File Transfer to Dublin Release Lab No. SDF-OTH-71	Rev 7	05/02/2007

Life Cycle Support documentation

Document	Version	Date
IBM DB2 Content Manager Enterprise Edition V8.4 Lifecycle document	Issue 0.9	February 28, 2008
IBM DB2 Content Manager Enterprise Edition V8.4 Flaw Remediation	Issue 0.3	January 16, 2008

Test documentation

Document	Version	Date
IBM® DB2® Content Manager Enterprise Edition v8.4 FP1A Security Related Test Plan	Issue 0.15	5 November 2008
IBM® DB2® Content Manager Enterprise Edition v8.4 FP1A Security Related Test Cases	Issue 0.13	5 November 2008

The actual test results have been submitted to the evaluation team in various log files.

Vulnerability Assessment documentation

Document	Version	Date
IBM DB2 Content Manager for Enterprise Edition Version 8.4 FP1A Vulnerability Analysis	Issue 0.7	19 November 2008
IBM DB2 Content Manager for Enterprise Edition Version 8.4 FP1A Vulnerability Analysis Supplement Security of Function & Misuse Analysis	Issue 0.8	20 October 2008

Security Target

Document	Version	Date
IBM® DB2® Content Manager Enterprise Edition V8.4 Security Target	Version 1.0	22 December 2008

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team.

8.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function tested. The scope of the developer tests included all the

TSFI. The testing covered the security functional requirements in the ST including: Security audit, User data protection, Identification and authentication, Security management, and Protection of the TSF. All security functions were tested and the TOE behaved as expected. The evaluation team determined that the developer's actual test results matched the vendor's expected results.

8.2 Evaluation Team Independent Testing

The evaluation team re-ran the entire automated test suite and a subset of the of the vendor's manual tests. In addition to re-running the vendor's tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the vendor's test suite, or areas where the ST did not seem completely clear. All were run as manual tests.

The vendor provided the TOE software and the necessary computers, hubs, and cabling for the test environment.

The following hardware is necessary to create the test configuration:

- TOE Hardware
    - For Windows - IBM PC, Intel Pentium 4 3.0 GHz, CD-ROM reader (for installation), 40GB Hard Disk, 2GB memory, and network adapter card.
    - For AIX - RS Power 4+ or 5 processor, CD-ROM reader (for installation), 40GB Hard Disk, 4GB memory, and network adapter card.
    - For z/Linux – zOS/390
- IT Environment Hardware
    - For CM Clients - IBM PC, Intel Pentium 4 3.0 GHz, CD-ROM reader (for installation), 40GB Hard Disk, 2GB memory, SVGA display (800 x 600 resolution and 256 color mode), and network adapter card.
    - Hub, Ethernet router, CAT 5e cabling, and any other items required to create a functional Ethernet network environment.

The following software is required to be installed on the machines used for the test:

TOE	Operating System	Database	WebSphere Application Server	Encryption Module (in the Library Server and Resource Manager)
IBM® DB2® Content Manager Enterprise Edition V8.4 FP1A	Windows Server 2003 SP2	DB2 Enterprise Server Edition V9.1 FP3 (64bits)	WebSphere Application Server V6.1.0.11(32bits)	Encryption Module IBM Crypto for C (ICC) version 1.4.5
IBM® DB2® Content Manager Enterprise Edition V8.4 FP1A	AIX 5.3 (64bits) Level 5003-05-02 pSeries	DB2 Enterprise Server Edition V9.1 FP3 (64bits)	WebSphere Application Server V6.1.0.11(32bits)	Encryption Module IBM Crypto for C (ICC) version 1.4.5

TOE	Operating System	Database	WebSphere Application Server	Encryption Module (in the Library Server and Resource Manager)
IBM® DB2® Content Manager Enterprise Edition V8.4 FP1A	Linux (zSeries) Red Hat Enterprise Linux Version 4 update 5 (64bits)	DB2 Enterprise Server Edition V9.1 FP3 (64bits)	WebSphere Application Server V6.1.0.11(32bits)	Encryption Module IBM Crypto for C (ICC) version 1.4.5

The following software will be required to be installed on the client machines used for the test:

TOE	Operating System
Content Manager Client for Windows CM8.4 FP1A	Windows 2003 SP2

In addition, the following software is required for the automated test scripts:

- Microsoft Visual C++ .net 2005 (same for the server & client)
- IBM Rational Functional Tester v7.0.1
- IBM Rational Test Manager v7.0.1
- IBM Rational Robot v7

In addition to developer testing, the evaluation team conducted its own suite of tests, which were developed independently of the sponsor. These also completed successfully.

8.3 Vulnerability Testing

The evaluators developed vulnerability tests to address the Protection of the TSF security function, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no vulnerabilities in the specific functions provided by the TOE.

9 Evaluated Configuration

The physical boundaries of the TOE are defined by the operating environment that each component of the TOE requires for effective operation. The operating environment includes the operating system, database, cryptographic provider, web application server, and system clock used to provide the timestamp used by the TOE. The TOE is a data management system comprised of the applications required for the correct enforcement of the security functions. The TOE utilizes an underlying database (DB2 Enterprise Server) that is part of the TOE's operating environment for data storage and protection. The TOE is intended to be distributed in a closed environment which has the security mechanisms that can be used to protect the data transmission and communication between the TOE components as deemed necessary.

The TOE components have the software dependencies on the IT environment as described below.

	Operating System	Additional Software
Client for Windows 8.4		
Windows	Windows Server 2003 Standard or Enterprise Edition *(32-bit)* or with SP1 or SP2 Windows Server 2003 R2 *(32-bit)* or with SP2 Windows XP Professional *(32-bit)* or with SP2 Windows Vista Business, Ultimate, or Enterprise Edition (*32-bit*)	Database Client if database is on a different machine: DB2 Run-Time Client V9.1 FP 3 *(32-bit)*
Enterprise Edition Server v8.4 (Library Server and Resource Manager)		
AIX	AIX® 5L 5.2 (*64-bit*) (Maintenance level 9, 10) AIX 5L 5.3 (*64-bit*) (Maintenance level 5, 6, 7) AIX 6.1	DB2 Enterprise Server Edition V9.1 FP3 *(32- or 64-bit)* Encryption Module (in the Library Server and Resource Manager): IBM Crypto for C (ICC) version 1.4.5 WebSphere Application Server V6.1.0 *(32- or 64-bit)* Fix Pack 11 or later WebSphere Application Server Network Deployment V6.1.0 *(32- or 64-bit)* Fix Pack 11 or later Database Client if database is on a different machine: DB2 Run-Time Client V9.1 FP 3 *(32-bit)*
Solaris	Solaris 9 *(64-bit)* Solaris 10 *(64-bit)*	DB2 Enterprise Server Edition V9.1 FP3 *(32- or 64-bit)* Encryption Module (in the Library Server and Resource Manager): IBM Crypto for C (ICC) version 1.4.5 WebSphere Application Server V6.1.0 *(32- or 64-bit)* Fix Pack 11 or later WebSphere Application Server Network Deployment V6.1.0 *(32- or 64-bit)* Fix Pack 11 or later Database Client if database is on a different machine: DB2 Run-Time Client V9.1 FP 3 *(32-bit)*
Linux	Red Hat Enterprise Linux AS/ES/WS 4.0 *(32- or 64-bit)* Kernel 2.6.9-5 (update 3) Red Hat Enterprise Linux AS/ES/WS 5.0 *(32- or 64-bit)* Kernel 2.6.18-8.el5xen SUSE Linux Enterprise Server 9 *(32- or 64-bit)* Kernel 2.6.5-7.97 (SP3) SUSE Linux Enterprise Server 10 SP1 *(32- or 64-bit)* Kernel 2.6.16.21-0.8-default	DB2 Enterprise Server Edition V9.1 FP3 *(32- or 64-bit)* Encryption Module (in the Library Server and Resource Manager): IBM Crypto for C (ICC) version 1.4.5 WebSphere Application Server V6.1.0 *(32- or 64-bit)* Fix Pack 11 or later WebSphere Application Server Network Deployment V6.1.0 *(32- or 64-bit)* Fix Pack 11 or later Database Client if database is on a different

		machine: DB2 Run-Time Client V9.1 FP 3 *(32-bit)*
z/Linux	Red Hat Enterprise Linux AS/ES/WS 4.0 *(64-bit)* Kernel 2.6.9-5 (update 3) Red Hat Enterprise Linux AS/ES/WS 5.0 *(64-bit)* Kernel 2.6.18-8.el5xen SUSE Linux Enterprise Server 9 *(64-bit)* Kernel 2.6.5-7.97 (SP3) SUSE Linux Enterprise Server 10 SP1 *(64-bit)* Kernel 2.6.16.21-0.8-default	DB2 Enterprise Server Edition V9.1 FP3 *(32- or 64-bit)* Encryption Module (in the Library Server and Resource Manager): IBM Crypto for C (ICC) version 1.4.5 WebSphere Application Server V6.1.0 *(32- or 64-bit)* Fix Pack 11 or later WebSphere Application Server Network Deployment V6.1.0 *(32- or 64-bit)* Fix Pack 11 or later Database Client if database is on a different machine: DB2 Run-Time Client V9.1 FP 3 *(32-bit)*
Windows	Windows Server 2003 Standard or Enterprise Edition *(32-bit)* or with SP1 or SP2 Windows Server 2003 R2 *(32-bit)* or with SP2	DB2 Enterprise Server Edition V9.1 FP3 *(32- or 64-bit)* Encryption Module (in the Library Server and Resource Manager): IBM Crypto for C (ICC) version 1.4.5 WebSphere Application Server V6.1.0 *(32- or 64-bit)* Fix Pack 11 or later WebSphere Application Server Network Deployment V6.1.0 *(32- or 64-bit)* Fix Pack 11 or later Database Client if database is on a different machine: DB2 Run-Time Client V9.1 FP 3 *(32-bit)*
System Administration Client		
AIX	AIX® 5L 5.2 (*64-bit*) (Maintenance level 9, 10) AIX 5L 5.3 (*64-bit*) (Maintenance level 5, 6, 7) AIX 6.1	Database Client if database is on a different machine: DB2 Run-Time Client V9.1 FP 3 *(32-bit)*
Solaris	Solaris 9 *(64-bit)* Solaris 10 *(64-bit)*	Database Client if database is on a different machine: DB2 Run-Time Client V9.1 FP 3 *(32-bit)*
Linux	Red Hat Enterprise Linux AS/ES/WS 4.0 *(32- or 64-bit)* Kernel 2.6.9-5 (update 3) Red Hat Enterprise Linux AS/ES/WS 5.0 *(32- or 64-bit)* Kernel 2.6.18-8.el5xen SUSE Linux Enterprise Server 9 *(32- or 64-bit)* Kernel 2.6.5-7.97 (SP3) SUSE Linux Enterprise Server 10 SP1 *(32- or 64-bit)* Kernel 2.6.16.21-0.8-default	Database Client if database is on a different machine: DB2 Run-Time Client V9.1 FP 3 *(32-bit)*
Windows	Windows Server 2003 Standard or Enterprise Edition *(32-bit)* or with SP1 or SP2 Windows Server 2003 R2 *(32-bit)* or with SP2 Windows XP Professional *(32-bit)* SP2	Database Client if database is on a different machine: DB2 Run-Time Client V9.1 FP 3 *(32-bit)*

	Windows Vista Business, Ultimate, or Enterprise Edition *(32-bit)*	

The Content Manager installation package includes the following components that are excluded from the Content Manager TOE:

- DB2 Information Integrator for Content (II4C)—a separate product delivered along with the Content Manager product package to facilitate the development of user applications.
- eClient—a browser-based web client that runs on Mozilla and Internet Explorer.

Although included in the Content Manager package, these components are not installed with Content Manager and must be installed separately. They are not required in order for Content Manager to operate and do not contribute to the security functionality provided by Content Manager. They are therefore excluded from the TOE.

Content Manager can be configured to use an LDAP directory as an external repository for user accounts. This configuration option is not covered by the Content Manager evaluation. Similarly, while Content Manager supports extendible user authentication features (via Authentication User Exits and Custom Login User Exit), these features are not included within the scope of the evaluation.

10 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.3, dated August 2005; the Common Evaluation Methodology (CEM), Version 2.3, dated August 2005; and all applicable International Interpretations in effect on March 2007. The evaluation confirmed that the IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1a product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 extended, and assurance requirements (Part 3) for EAL4 Augmented with ALC_FLR.2. The details of the evaluation are recorded in the CCTL's evaluation technical report; Evaluation Technical Report for IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack1A, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1a Security Target, Version 1.0, 22 December 2008.

The Validators followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures. The Validators observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The Validators therefore conclude that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL.

10.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1A product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

10.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 4 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control, and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. The evaluation team ensured the procedure included automated support to control and track changes to the implementation representation. The procedures reduce the risk that security flaws exist in the TOE implementation or TOE documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from IBM.

10.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 4 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification, the discrepancy between the developer master copy and the version received, and the detection of attempts to masquerade as the developer.

The evaluation team followed the IBM DB2 Content Manager Enterprise Edition Version 8 Release 4 Planning and Installing Your Content Management System to test the installation procedures to ensure the procedures result in the evaluated configuration.

10.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification, a high-level design document, a low-level design document, and a security policy model. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

10.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the guidance documents in describing how to securely administer the TOE. The IBM DB2 Content Manager Enterprise Edition Version 8 Release 4 Planning and Installing Your Content Management System and the IBM DB2 Content

Manager Enterprise Edition System Administration Guide Version 8 Release 4 were assessed during the design and testing phases of the evaluation to ensure it was complete.

10.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL4, augmented with ALC_FLR.2, ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The evaluation team ensured the procedures described the life-cycle model and tools used to develop and maintain the TOE. To support the ALC evaluation, the evaluation team performed a Life Cycle audit at the IBM facility in San Jose, CA. During the audit, the evaluation team witnessed the use of the security measures as described in the Life Cycle documentation and sampled records created by using the security procedures.

In addition to the EAL4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that systematic procedures exist for managing flaws discovered in the TOE.

10.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation Team applied each EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team exercised the complete Vendor test suite and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

10.8 Vulnerability Assessment Activity (AVA)

The Evaluation Team applied each EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer vulnerability analysis, the evaluation team's misuse analysis, the evaluation team's vulnerability analysis, and the evaluation team's performance of penetration tests.

10.9 Summary of Evaluation Results

The Evaluation Team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation Team's performance of the entire set of the vendor's test suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

11 Validator Comments/Recommendations

The validation team observed that the evaluation was performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR.

The validation team, therefore, recommends that the evaluation and Pass result for the identified TOE be accepted.

12 Security Target

The Security Target is identified as IBM® DB2® Content Manager Enterprise Edition V8.4 FP1A Security Target, Version 1.0, dated 22 December 2008. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE SFRs and IT Environment SFRs. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 4 augmented with ALC_FLR.2.

13 Glossary

The following definitions are used throughout this document:

ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
IBM	International Business Machines
ID	Identification
IT	Information Technology
NIST	National Institute of Standards and Technology
PC	Personal Computer
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target

TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
XML	Extensible Markup Language

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 2.3, August 2005.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security Functional Requirements, Version 2.3, August 2005.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security Assurance Requirements, Version 2.3, August 2005.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005.

[5] IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1A Final Proprietary ETR – Part 2, Version 2.0 dated 19 November 2008 and Supplemental Team Test Report, Version 2.0, 21 November 2008.

[6] IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1A Final Proprietary ETR – Part 1, Version 2.0, 18 November 2008.

[7] IBM® DB2® Content Manager Enterprise Edition V8.4 FP1A Security Target, Version 1.0, 22 December 2008.

[8] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.