National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

IBM® DB2® Document Manager V8.4 FP1

Report Number: CCEVS-VR-VID10221-2009
Dated: 30 January 2009
Version: 1.2

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® Document Manager V8.4 FP1.

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® Document Manager V8.4 FP1 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 3 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® Document Manager V8.4 FP1. Document Manager provides the capability to manage controlled documents, such as standard operating procedures, engineering drawings, work instructions, and material safety data sheets, throughout the lifecycle of the documents.

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 Validators conclude 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® Document Manager V8.4 Fix Pack 1
Protection Profile	Not applicable
ST	IBM® DB2® Document Manager V8.4 Fix Pack 1 Security Target, Version 1.0, 8 January 2009
Evaluation Technical Report	Evaluation Technical Report For IBM® DB2® Document Manager V8.4 FP1 (Non-Proprietary), Version 1.0 21 November 2008, Part 2 (Proprietary), Version 2.0 23 December 2008

Item	Identifier
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 3 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 Document Manager (DM) 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 be configured to track an item's life cycle activities for items defined in a controlled class.

The following activities can be configured to be logged in the "Lifecycle History" activity log for the items defined in controlled classes:

- Add – Item was created.
- Checkin – Item was checked into the IBM Content Manager (CM) library.
- Checkout – Item was checked out from the CM library.
- Copy – Item was copied out from the CM library (that is, a copy was made of the library item, but the item was not checked out).
- Delete – Item was deleted from the CM library.
- Library Update – Item was updated in the CM library (i.e., updates the library with a copy of a checked-out item that is currently being edited. This update will check in a new version and draft of the document, then check it out again)
- Markup added – A new markup item was associated with the item.

- Modify properties – Item properties were modified.
- Notification – An email or instant message notification was sent for the item. Notifications may be requested after other activities have completed like a Rendition, Revise, etc.
- Print – Item has been printed.
- Process – route actions – A user-defined CM document routing action has been executed on the item from DM. User-defined actions are those actions that are defined as part of the CM document routing process. This only records user-defined document routing actions executed from within DM.
- Process – system actions – A system-defined CM document routing action has been executed on the item from DM. System-defined actions include the CM document routing actions: Change Route, Change Priority, Change Owner, Terminate Route, Activate and Suspend and the DM document routing commands Change Details, Select Route and Define Route. This only records system-defined document routing actions executed from within DM.
- Record Management – A Record Management operation was executed on the item. For example, declaring the item as an item of record. This only records Record Management operations executed from within DM.
- Rendition – Item has been rendered into another format.
- Revise –Item has been revised. Updates were approved and a new "revision" was created.
- Transition – Item has been transitioned to a different state. (DM Lifecycle)
- View – Item has been viewed.

A number of these activities are associated with controlled operations within the scope of the DM Access Control SFP and can be configured to be logged when users perform controlled operations on controlled documents.

The desktop client provides the command that allows the authorized users to review the log records. The entries in the activity logs include the following information:

- item version;
- date and time the operation was executed (the date and time are obtained from the IT environment);
- activity;
- additional activity-specific details;
- user's login name (subject identity);
- group; and
- role under which the operation was allowed.

Note that the TOE records only activities that actually occur—it does not record failed attempts to perform an activity. The activity logs are stored and protected by the underlying OS of the TOE server component.

3.2 Identification and authentication

The TOE presents a login screen to users of the Desktop when it is first started. The user identity and password are passed through to the IT environment for identification and authentication prior to granting any further access to the TOE. The TOE enforces the identification and authentication decision received from the IT environment and ensures the user does not gain access to the TOE if identification and authentication fail. The TOE associates the user identity with the current active session and uses this identity and the user's document management roles to enforce the access control policy on documents.

The Desktop client can be configured by the administrator to require the end user to re-login if idle for longer than a configurable interval. The TOE also provides a mechanism to lock user accounts if a configured number of consecutive failed login attempts occur. However, the underlying CM system provides a stronger mechanism (since accounts are locked until the authorized administrator unlocks them), so guidance documentation advises using the CM account lock-out mechanism rather than the mechanism provided by the TOE.

3.3 User data protection

The TOE enforces a role-based access control policy that controls the actions users can perform on documents, based on the roles the user is associated with and the life cycle stage of the document. Users of the TOE are identified and authenticated by the IT environment before any access to the TOE is granted. The TOE defines document management roles, and associates those roles with users and groups that are defined in the IT environment. The roles a user is associated with determine what commands a user can perform. Roles are also associated with the various states in which a document type can exist. The document life cycle defines how the document transitions through its various states. A document life cycle stage is the current state of the document and the transitions that apply to the document in its current state. The TOE ensures the user has an appropriate document management role and that the requested operation is valid for the current life cycle stage of the document before allowing a requested operation to be performed. The Desktop tier and the Server and Services tier work together to implement the role-based access control policy.

The IT environment (specifically, the IBM DB2® CM component of the content repository tier) enforces its own access control policy on the items stored within the content repository, including the items the TOE presents to users as documents. Access to these items is governed by the item's Access Control List (ACL) that identifies the user and the access allowed. The IT environment uses privileges to define what operations a user is allowed to perform on the items. The Library Server component verifies that the user has the required privilege and the ACL associated to the requested item grants access. This access is enforced regardless of the commands a TOE user might be granted by their role assignment. That is, CM access control is always enforced, and DM access control adds

another layer of control. DM's role-based access controls cannot grant additional access to CM items, they can only further restrict the access a user is otherwise granted by the CM access controls.

3.4 Security management

The TOE supports a single security management role of administrator. Any user not granted the administrator role that logs into the system administration client application (i.e., Designer) has no ability to perform security management functions and can only view the TOE configuration. Note that a DM administrator is actually a CM administrator—the TOE does not define users or groups but instead relies on the underlying CM repository to manage users and groups, including administrative users.

Administrators are able to perform the following functions provided by Designer:

- Create and modify document management roles, including associating users and groups with roles
- Create and modify document states, including associating document management roles with states
- Create and modify classes, including associating Document Lifecycle Templates and states with classes
- Define a document life cycle, including all the states the document can have in the life cycle and the manner in which the document transitions from one state to another
- Define the initial life cycle state that a document will be in when it is first created. This value cannot be overridden
- Modify the parameters used to control the session termination function.

4 Threats and Assumptions

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 threats that the TOE is intended to counter, the assumptions made on the TOE and operational environment, and the organizational security policies with which the product is to comply.

Following are the threats against the TOE and its environment as identified in the Security Target.

- A user may perform unauthorized actions on the TOE that go undetected.
- An unauthorized user may gain access to the TOE and its resources in order to bypass, deactivate, or tamper with TOE security functions.
- An unauthorized user may gain access to objects maintained by the TOE in order to modify or destroy them.

Following are the assumptions identified in the Security Target:

- It is assumed the TOE will be located within controlled facilities that will prevent unauthorized physical access and modification.
- 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 environments are configured in accordance with the manufacturer's installation guides and in a secure manner that protects them from any unauthorized users or processes and protects the communication between components.

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 3 augmented in this case).
- DM works with IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1a to manage controlled documents throughout their lifecycle. Typical controlled documents include standard operating procedures, engineering drawings, work instructions, and material safety data sheets. DM provides relationship management of related documents and manages the various states and transitions that occur throughout a document's lifecycle, from creation to disposition or destruction.
- The TOE uses special-purpose, and evaluated, APIs (i.e., DM Client 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., DM desktop, Designer, or Item Loader, etc.) are also considered to be outside of the evaluated configuration.

6 Architectural Information[1]

The DM system is built on a three-tiered computing model as follows:

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

- **Content Repository tier—**provides a foundation for managing, accessing, and integrating critical business information on demand. All DM documents are stored within the underlying CM system. DM does not require additional databases or tables to be created in this case. The CM repository incorporates an underlying database, the IBM DB2 Universal Database™ to manage documents and information. This environment consists of a CM library server and one or more resource managers. It should be noted that CM works with "items", and that DM documents are one type of item that may be managed in the repository. The library server is responsible for maintaining and controlling information about items in the repository. Access control of the item and item attributes are managed by the library server and the resource manager stores the associated file. This tier is part of the TOE's operating environment, but not part of the TOE.
- **Document Manager Server and Services tier—**the middle tier of the system. This tier comprises several components, some of which are automated services that run at designated intervals. These components interact directly with the Content Repository tier and the Document Manager Desktop tier (see below). The four primary components of the Server and Services tier are:
  - Library Objects (also referred to as DM Server)—control communication with the content repository. All information, including configuration, compound document, rendition, and other DM specific information are stored in the repository.
  - Cache Manager—controls the information (in the form of cache objects) stored in the cache, such as user, document state and class, and menu data. Cache objects are small files that contain configuration information, such as menus, actions, dialogs and folders. The cache files are stored on the Document Manager Server. As changes are made to the DM configurations using the Designer (a tool used to configure the Desktop—see below), Cache Manager updates those configurations in the repository and in the cache files that are stored on the Document Manager Server. The use of cache objects enhances Document Manager Desktop performance by reducing the resource utilization that occurs in client-server applications. Note that Cache Manager runs as a Windows service, is configured from the DM Service Manager, and is thus included in the "Services" bulleted item below. However, it differs from the other DM services in that it provides the generic service of creating and updating the DM cache, which is used by the other DM services. Thus it is described separately here.
  - Services—control specialized task processing. The DM services are specialized applications that run as Windows services. These services comprise: Lifecycle Services; Notification Services; Rendition Services; Print/Plot Services; Automation Services; Alarm Manager; and Cache Manager (see separate bulleted item above).
  - Client Software Delivery component—controls software installation and updates to the Document Manager Desktop.

- **Document Manager Clients tier**—consists of the following five components:
  - Desktop—a client application that provides a configurable environment from which the user can:
    - Organize the workspace
    - Check out and check in, copy, view, and print items in the repository
    - Transition items in the life cycle
    - Integrate with desktop applications to work directly with items in the repository.
  - Application Integration—the DM Desktop exposes DM features from within other applications through application integration. DM supports integration with the Microsoft Office suite (Word, Excel, PowerPoint, and Outlook), Lotus Notes, AutoCAD, Microstation, AutoVue and other viewing applications. Note that users cannot interact with the TOE directly from or via end user applications. When an application is "integrated" with the Desktop, it provides a means for the user to access the application from the Desktop and to use the application to work with documents maintained within the TOE. The user still needs to login to the Desktop before being able to access an integrated application from the Desktop.
  - Designer—a system administration client application used to customize the Desktop for users and groups. The authorized administrator is able to create Desktop templates and assign these to users and groups. The Desktop template is used to configure the DB2 Document Manager Desktop for end users. Menus, views, searches, application integration profiles, and native library folder displays are among the many Desktop objects that can be configured and assigned to a user or group via the Desktop template. Desktop templates can be assigned at the system, group, or user level. If a user or group has not been assigned to a Desktop template, the user or group automatically uses the Default Template configuration. Users and groups must be assigned to other templates in order for their DB2 Document Manager Desktop to use the configuration of that template.

    The Designer enables the authorized administrator to configure the Document Manager environment and the Desktop. After the administrator deploys the Desktop to the users, any changes made by the administrator using the Designer are automatically pushed to the Desktop. The Desktop can be configured to implement updates when the next user action is invoked[2] or at the start of the user's next login session

    Note: *The Designer does not require users to identify or authenticate themselves before accessing its capabilities. By default, Designer is installed on the same computer as the DM Server component. This computer is assumed to be located within a controlled access environment that protects it from*

[2] This option is not recommended as it has a significant impact on performance, since the cache is checked against the cache server on every attempted operation.

unauthorized physical access and modification. In addition, during initial configuration of the TOE, the TOE administrator should use Designer to configure a Desktop template that includes the "Configure" command and that is assigned only to a TOE administrator role. Following the initial configuration of the TOE library and the administrator Desktop template, Designer should always be run via the "Configure" command from this administrator Desktop client. This will ensure that the administrator must be identified and authenticated before accessing other TOE capabilities.

- Item Loader—simplifies the batch loading of items into the repository. The Item Loader not only adds items, but also provides the capability to maintain compound relationships, set access control, load item profile information, add items to specific folders, as well as submit items for life cycle, rendition, or print or plot processing. The Item Loader allows the user to set up default values for specific item and version properties, the access control list, keywords, and folders. Using the Desktop, the user can override these default values for individual selected files.

  The Item Loader has the technology to scan documents for reference files and automatically add the reference files and maintain those relationships within the content repository. It can automatically detect relationships between some types of compound documents such as CAD reference files and Object Linking and Embedding (OLE) linked files like spreadsheets linked to word processing documents. The Item Loader supports parent-child links, peer-to-peer links and dynamic links.

- Client API—the COM-based Client API can be used to develop DM plug-ins, application integrations, and completely new applications. It comprises a set of COM objects, interfaces and properties that support early and late binding. It is delivered with the Desktop Client in a self-registering Windows dynamic link library.

The following diagram depicts the components of DM as described above in the preceding section.

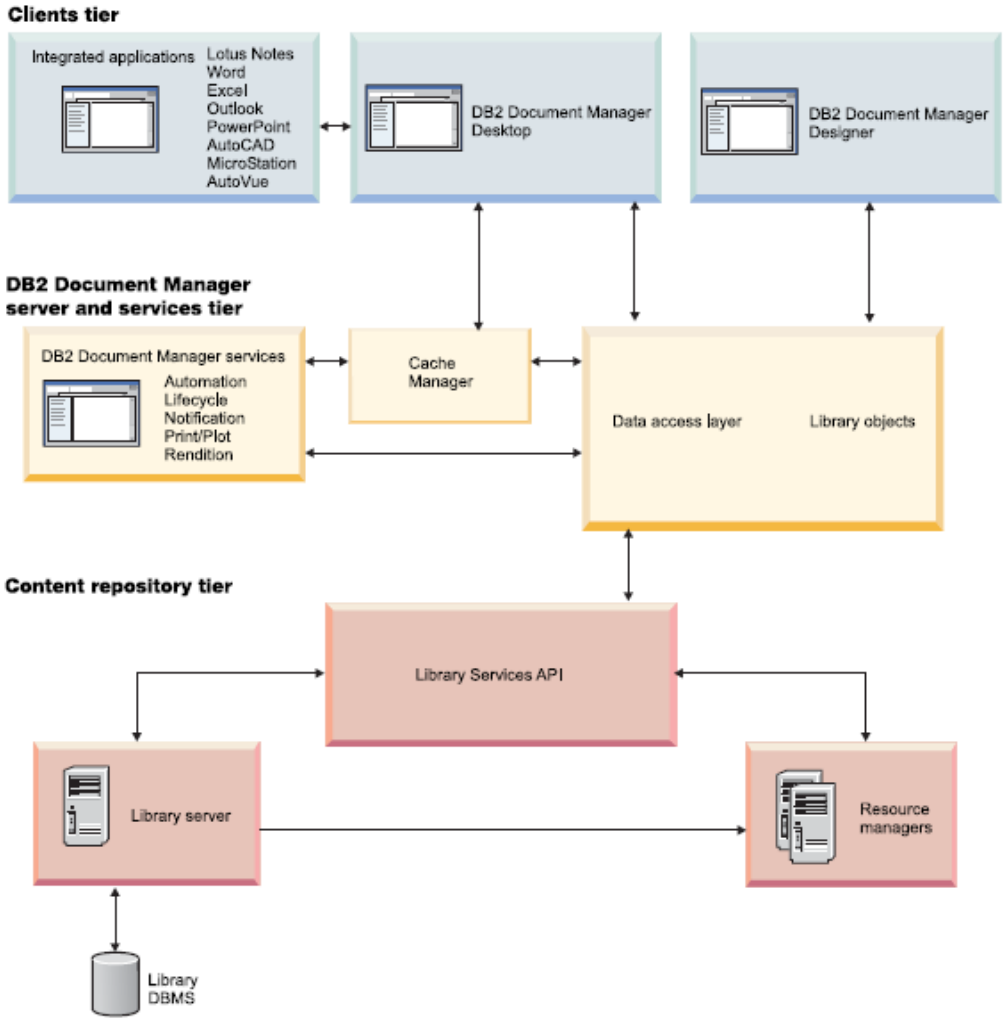

Figure 1. Three-tiered architectural model of the DB2 Document Manager system

All components within the “DB2 Document Manager server and services tier” and the “DB2 Document Manager Desktop” and “DB2 Document Manager Designer” components in the “Clients tier” are TOE components. Within the “Integrated applications” component in the “Clients tier”, the listed applications (Lotus Notes, Word, Excel, etc.) are in the IT environment. All components in the “Content repository tier” are also in the IT environment. Note also that the “Data access layer” encapsulates the “Client Software Delivery” component.

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 Document Manager Version 8.4 Fix Pack 1 Security High-level Functional Specification And Design	Issue 0.9	22 October 2008
IBM DB2 Document Manager Version 8.4 Fix Pack 1 Representation Correspondence (ADV_RCR)	Issue: 0.3	27 August 2008

Guidance documentation

Document	Version	Date
IBM DB2 Document Manager System Administration Guide Version 8 Release 4Release 4		
Addendum to the IBM DB2 Document Manager System Administration Guide	Version 1.1	3 October 2008
DB2 Document Manager Client Application Programming Interface Reference Version 8 Release 4		

Configuration Management documentation

Document	Version	Date
IBM DB2 Document Manager v8.4 Configuration Management	Issue 0.7	June 24 2008
IBM DB2 Document Manager Submitted documentation list		January 16 2008

Delivery and Operation documentation

Document	Version	Date
IBM DB2 Document Manager V8.4 Delivery Operation and Guidance	Issue 0.6	16 January 2008
IBM DB2 Document Manager Planning and Installing Your Content Management System Version 8 Release 4	Version 8 Release 4	
DSW Secure Media Delivery (SMD)	v1.2	
Download Director Command Line Client (DDP) User Guide	Version 3.01	16 August 2004
Tequila for eSD and Golden Master File Transfer to Dublin Release Lab No. SDF-OTH-71	Rev 7	2 May 2007

Life Cycle Support documentation

Document	Version	Date
IBM DB2 Document Manager V8.4 Lifecycle document	Issue 4.0	8 March 2008
IBM DB2 Document Manager V8.4 Flaw Remediation	Issue 1.1	

Test documentation

Document	Version	Date
IBM DB2 Document Manager Version 8.4 FP1 Security Functions Test Plan	Issue 2.16	7 November 2008
IBM DB2 Document Manager Version 8.4 FP1 Security Functions Test Case	Issue 2.16	7 November 2008

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

Vulnerability Assessment documentation

Document	Version	Date
IBM DB2 Document Manager Version 8.4 Fix Pack 1 Vulnerability Analysis	Issue 0.5	October 23 2008

Security Target

Document	Version	Date
IBM® DB2® Document Manager V8.4 Fix Pack 1 Security Target	Version 1.0	8 January 2009

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, and Security management. 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 ran a subset 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
  - DM Server and Services
    - IBM PC, Intel Pentium 1 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
  - DM Desktop Client
    - 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.
- IT Environment Hardware
  - IBM CM Repository
    - IBM PC, Intel Pentium 4 3.0 GHz, CD-ROM reader (for installation), 40GB Hard Disk, 2GB memory, and network adapter card.
  - TAM/WebSEAL (Intermediate Server)
    - IBM PC, Intel Pentium 4 3.0 GHz, CD-ROM reader (for installation), 40GB Hard Disk, 2GB memory, and network adapter card.
- Test Hardware
  - No specific test hardware is required
  - 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	Environment Requirements
IBM DB2® Document Manager V8.4 FP1	Windows Server 2003 SP2	IBM® DB2® Content Manager Enterprise Edition V8.4 FP1 in its evaluated configuration, including 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, Microsoft Outlook Express

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

TOE	Operating System
Document Manager Client	Windows XP SP2 Microsoft .NET Framework 2.0, Cimmetry AutoVue 19.1c1, Microsoft Office 2003 SP2

- The following software is required to be installed on the Intermediate Server; Windows 2000 SP2 and TAM/WebSEAL.

All tests 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, IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1a in its evaluated configuration, and system clock used to provide the timestamp used by the TOE. The TOE provides the capability to manage controlled documents, such as standard operating procedures, engineering drawings, work instructions, and material safety data sheets, throughout the lifecycle of the documents. It enforces a role-based policy that controls what operations users can perform on documents, based on the user's role. DM relies on IBM® DB2® Content Manager Enterprise Edition V8.4 Fix Pack 1a to act as a content repository for DM documents. The TOE is intended to be distributed in a closed environment that has the security mechanisms that can be used to protect the data transmission and communication between the TOE components as deemed necessary.

The following table identifies the IT environment requirements for the DM Server and Services Tier components.

OS	**DB2 + fix packs**	**II4C C++ Connector**
Windows Server 2003, Service Pack 2 Windows Server 2003, Service Pack 1 Windows Server 2003, R2 Service Pack 2 Windows Server 2003, R2 Windows 2000 Advanced Server, Service Pack 4 Windows 2000 Server, Service Pack 4	UDB and SDK V9.1 FP3	8.4 Fix pack 1

The following table identifies the IT environment requirements for the DM Clients Tier components:

Software	**Level**
Windows OS	Windows Vista (Business, Ultimate, and Enterprise Editions (x86 32-bit)) Windows XP Professional, Service Pack 2 Windows XP Professional, Service Pack 1 Windows XP Professional Windows 2000 Professional, Service Pack 4 Windows Server 2003, Service Pack 2 Windows Server 2003, Service Pack 1 Windows Server 2003, R2 Service Pack 2 Windows Server 2003, R2 Windows 2000 Advanced Server, Service Pack 4 Windows 2000 Server, Service Pack 4
Internet Explorer	**On Microsoft Windows Vista and Microsoft Windows XP systems:** Microsoft Internet Explorer 7 **On all supported Microsoft Windows systems:** Microsoft Internet Explorer 6

The following table identifies supported levels of applications that can be integrated with the DM Desktop.

Software	**Level**
Adobe Acrobat (Distiller)	7.0.9 and 8.1.1
Autodesk AutoCAD	2006, 2007, 2008, 2008 Service Pack 1
Bentley MicroStation J, MicroStation 8, MicroStation 8 XM	J, 8, 8XM
Cimmetry AutoVue client	18, 19.1, 19.1 Service Packs 1 and 2

Lotus Notes	6,5,7,8
Microsoft Office XP, 2003, 2007, 2007 Service Pack 1 • Microsoft Excel • Microsoft Outlook • Microsoft PowerPoint • Microsoft Word	Microsoft Office XP, 2003, 2007, 2007 Service Pack 1
Parametric Technology Corporation (PTC) Arbortext Editor	5.3

The TOE utilizes the CM repository, which is part of the IT environment, to store and manage documents. DM Desktop can be installed on the same computer as DM Server, which means it can be installed on the same computer as DM Designer (Designer is installed with DM Server). DM Desktop can also be installed on a separate computer from the DM Server, which is the most common configuration.

The IT environment should provide the secure channel for communication between the TOE components or between the TOE and Content Manager. In the Windows operating environment, Microsoft DCOM can be configured to use an authentication level of "packet privacy" to encrypt the content of all DCOM network packets or DM .NET Remoting can be configured to send and receive messages over secure HTTP - HTTPS.

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® Document Manager V8.4 Fix Pack 1 product is compliant with the Common Criteria Version 2.3, functional requirements (Part 2), Part 2 extended, and assurance requirements (Part 3) for EAL3 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® Document Manager V8.4 Fix Pack 1, Part 1 (Non-Proprietary) and Part 2 (Proprietary). The product was evaluated and tested against the claims presented in the Document Manager V8.4 Fix Pack 1 Security Target, Version 1.0, 8 January 2009.

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 threats, policies, and assumptions, a statement of security requirements claimed to be met by the IBM® DB2® Document Manager V8.4 Fix Pack 1 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 3 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 3 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 Document Manager Version 8 Release 4 Planning and Installing Your Document 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 3 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 and a high-level design document. 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 3 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 Document Manager Version 8 Release 4 Planning and Installing

Your Document Management System and the IBM DB2 Document Manager 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 EAL 3, 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. 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 EAL 3 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 3 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 3 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® Document Manager V8.4 FP1 Security Target, Version 1.0, dated 8 January 2009. 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 3 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® Document Manager V8.4 Fix Pack 1 Final Proprietary ETR – Part 2, Version 2.0 dated 23 December 2008 and Supplemental Team Test Report, Version 1.0, 21 November 2008.

[6] IBM® DB2® Document Manager V8.4 Fix Pack 1 Final Proprietary ETR – Part 1, Version 1.0, 21 November 2008.

[7] IBM® DB2® Document Manager V8.4 FP1 Security Target, Version 1.0, 8 January 2009.

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