National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

IBM DB2® Content Manager Multiplatforms v8.2

Report Number: **CCEVS-VR-04-0081**
Dated: **December 22, 2004**
Version: **1.1**

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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Kathy Cunningham
NSA

Common Criteria Testing Laboratory

Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary 1
1.1 Evaluation Details 1
1.2 Interpretations 2
1.3 Threats to Security 2
2 Identification 3
2.1 ST and TOE Identification 3
2.2 TOE Overview 3
2.3 IT Security Environment 4
2.3.1 Logical Boundaries 4
3 Security Policy 5
4 Assumptions 5
4.1 Personnel Assumptions 5
4.2 Physical Assumptions 6
4.3 System Assumptions 6
5 Architectural Information 6
6 Documentation 7
7 IT Product Testing 8
7.1 Developer Testing 8
7.2 Evaluation Team Independent Testing 9
7.3 Evaluation Team Penetration Testing 9
8 Evaluated Configuration 9
9 Results of the Evaluation 10
10 Validator Comments/Recommendations 12
11 Annexes 12
12 Security Target 12
13 Glossary 13
14 Abbreviations 14
15 Bibliography 15

1 Executive Summary

The evaluation of IBM DB2® Content Manager Multiplatform v8.2 was performed by Science Applications International Corporation (SAIC) in the United States and was completed on November 23, 2004. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 2.1 and the Common Methodology for IT Security Evaluation (CEM), Version 1.0.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 1.0) for conformance to the Common Criteria for IT Security Evaluation (Version 2.1). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the IBM DB2® Content Manager Multiplatform v8.2 product by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 3 augmented with ALC_FLR.1) have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC.

1.1 Evaluation Details

Evaluation Completion: November 23, 2004

Evaluated Product: IBM DB2® Content Manager Multiplatform v8.2

Developer: IBM Corporation
555 Bailey Avenue
San Jose, CA 95161

CCTL:	Science Applications International Corporation Common Criteria Testing Laboratory 7125 Columbia Gateway Drive, Suite 300 Columbia, MD 21046
Validation Team:	Kathy Cunningham National Security Agency (NSA) 9800 Savage Rd Ft. Meade, MD 20755
Evaluation Class:	EAL 3 augmented with ALC_FLR.1
Completion Date:	November 23, 2004

1.2 Interpretations

The Evaluation Team determined that the following CCIMB Interpretations were applicable to this evaluation:

International Interpretations

003	Unique identification of configuration items in the configuration list, 2002-02-11
004	ACM SCP.*.1C requirement unclear, 2001-11-12
038	Use of 'as a minimum in C&P elements, 203-10-31
043	Meaning of "clearly stated" in APE/ASE OBJ.1, 2001-02-16
051	Use of 'documentation' without C&P elements, 2002-10-05
065	No component to call out security function management, 2001-07-31
084	Separate objectives for TOE and environment, 2001-02-16
085	SOF Claims additional to the overall claim, 2002-02-11
094	FLR Guidance Documentation Missing, 2001-07-31
103	Association of Access Control Attributes with Subjects and Objects, 2003-07-15
111	Settable Failure Limits are Permitted, 2003-10-31
201	"Other properties" in specified by assignment, 203-10-31
202	Selecting One or More items in a selection operation and using "None" in a assignment, 203-08-26

The Validation Team concluded that the Evaluation Team correctly addressed the interpretations that it identified.

1.3 Threats to Security

The Security Target does not identify any threats for the evaluated product.

2 Identification

2.1 ST and TOE Identification

ST: IBM DB2® Content Manager Security Target

TOE Identification: IBM DB2® Content Manager for Multiplatforms V8.2 + fix pack 6 for Sun Solaris 2.8, AIX® 5.1, Windows® 2000, and Windows XP

IBM DB2® Content Manager for Multiplatforms V8.2 GA for Linux RedHat 3.0, Linux SUSE 8

IBM DB2® Content Manager for Multiplatforms V8.2 + PTF UQ89832 for z/OS v1.3

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

Protection Profile (PP) Identification – The TOE does not claim conformance to a PP.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 1.0, August 1999.

2.2 TOE Overview

The TOE is a database software application that is comprised of the applications required for the correct enforcement of the security functions. The TOE utilizes an embedded database, DB2 Universal Database, and web applications through Websphere Application Server (WAS) interfaces, which are part of the environment. See figure 1 in Section 5 Architectural Information of this report.

The TOE, IBM DB2® Content Manager is a data management system (content management system) that provides a foundation for managing, accessing, and integrating critical business information that is stored within a database on demand. Content Manager is able to integrate all forms of data — document, Web, image, rich media — across diverse business processes and applications, including Siebel, PeopleSoft, and SAP, presenting the data in a integrated context for later use.

Enterprise-wide content integration

- Content Manager provides an integrated information framework for single-point access to all heterogeneous systems of content repositories.
- Content Manager includes content connectors to enable access to a broad range of IBM repositories, and allows connectors to be constructed for new target systems to support searching in both IBM and non-IBM content repositories as needed.

- Content Manager provides a federated connector as the common interface for content in multiple applications. The federated connector accesses individual connectors to allow any content sources (including non-IBM products) to be accessed with common APIs and components.

Supported operating systems

- Sun Solaris 2.8
- AIX® 5.1
- Windows® 2000
- Windows XP
- Linux RedHat 3.0
- Linux SUSE 8, and
- z/OS v1.3

2.3 IT Security Environment

The TOE security environment consists of the organizational security policies and usage assumptions as they relate to TOE. The TOE provides for a level of protection that is appropriate for IT environments that require control over what information is accessed by the users on the systems. It is suitable for use in both commercial and government environments. The organizational security policies enforced by the TOE are sufficient to mitigate and counter any implied threat to the assets protected by the TOE.

2.3.1 Logical Boundaries

The logical boundaries of the TOE can be described in the terms of the security functions that the TOE provides.

Audit: All security-related events within Content Manager are logged. These are tied to the user/administrator that performed the action, as well as the action performed, and the time it was performed. These audit records are stored in a central location where an authorized administrator can review them. Authorized non-administrative users can review the audit records generated for resources that they have been granted access. The IT environment provides the tools that are utilized by the TOE users to review the audit records.

Identification and Authorization: Content Manager requires the user to be identified and authenticated before any other actions can be performed. The user is required to provide a user name and password, which will be verified by the Library Server database table. If the verification is successful access into the TOE is granted.

User Data Protection: Access to the resources and its information is governed by the object's ACL that identifies the user and the privileges allowed. The Library Server verifies that the user has the required privilege and the ACL associated to the requested object grants access.

Security Management: System Administration Clients provides the authorized administrator the capability to manage the security-related functions and attributes, such as the audit function, management of users and their associated data.

TSF Protection: Content Manager provides various mechanisms to protect the integrity of the TSF data in transit and to enforce the access control policy ensuring that only authorized users with the appropriate privilege(s) are given access to the resources.

The Content Manager utilizes a resource security token to ensure that the access control information is protected from disclosure and modification when transmitted to the Resource Manager where the resource requested is stored. The security token contains the resource item ID, version ID, action to be performed, and a timestamp for when the access granted will expire.

3 Security Policy

The Security Target identified the following Security Policies for the evaluated product:

P.OBJ_ACCESS	The TOE must limit the access to, modification of, and destruction of the resource objects to those users that are authorized to access to the resource object.
P.ACCOUNTABILITY	Users of the system shall be held accountable for their security relevant actions within the system.
P.AUTH_USERS	Only those users who have been authorized to access the information within the TOE may access the TOE.
P.MANAGE	The TOE must provide authorized administrators with utilities to effectively manage the security-related functions of the system.
P.TRANSIT	The TOE must have the ability to protect system data during transmission between distributed parts of the TOE.

4 Assumptions

4.1 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

A.AUTH_DATA	Authorized users of the TOE will keep all their authentication data private.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The administrative personnel are not careless, willfully negligent, or hostile and

	will follow and abide by the instructions provided by the administrative guidance.
A.TRAINED_STAFF	Authorized TOE users and administrators are trusted to follow the guidance provided for the secure operation of the TOE

4.2 Physical Assumptions

The following physical assumptions are identified in the Security Target:

A.PROTECT	The components of TOE software critical to security policy enforcement must be located within controlled access facilities that will protect the TOE components from unauthorized physical access and modification.

4.3 System Assumptions

The following system assumptions are identified in the Security Target:

A.OS	It is assumed that the operating system has 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 system protects the TOE from any unauthorized users or processes
A.SYSTEM	The underlying environment will provide protection to the TOE and its related data and a reliable system time.

5 Architectural Information

The main components of the Content Manager include a Library Server, one or more Resource Managers, Client for Windows, System Administration Client, and a set of object-oriented application programming interfaces (APIs).

- The Library Server is the key component of the Content Manager system. The Library Server includes the DB2 Universal Database, however it should be noted that DB2 Universal Database is not part of the TOE. The Library Server manages the content metadata (resources) 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 Resource Manager stores the resources for Content Manager. The Client for Windows communicates directly with the Resource Manager using Internet protocols. Security tokens received from the Library Server are passed to Resource Managers from the client to provide assurance that the request has been authorized and the access control information has not been altered since leaving the Library Server.

- The System Administration Client oversees the entire Content Manager system. From the System Administration Client, an administrator performs various administrative functions, such as define 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 Client for Windows provides a user interface that enables the user to import documents into Content Manager, view them, work with them, store them, and retrieve them. The APIs associated with the Client for Windows are part of the TOE.
- The WebSphere Application Server (WAS) interface for the Resource Manager is another IBM product. WAS provides the Resource Manager access to web applications as a requested resource.

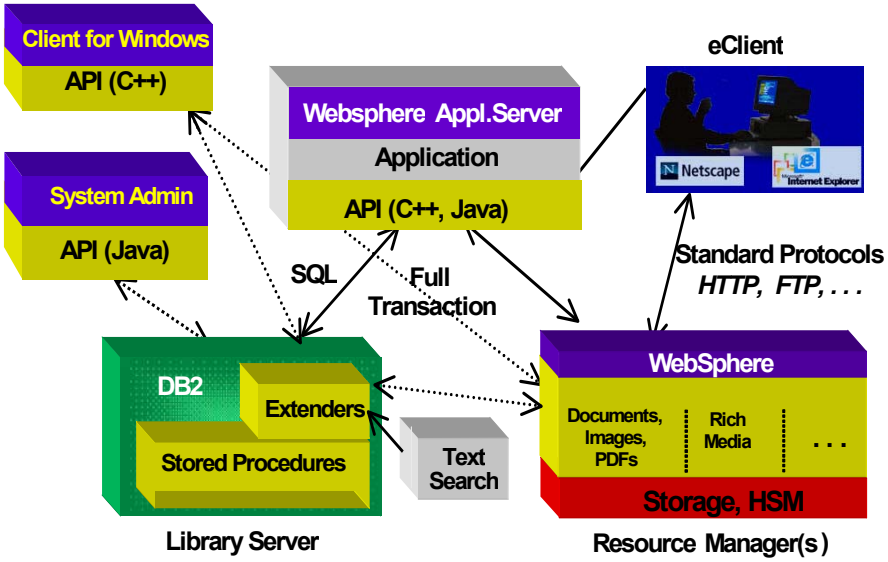

Figure 1: Content Manager Architecture

In figure 1 the TOE is shown in yellow.

6 Documentation

Purchasers of IBM DB2® Content Manager Multiplatform v8.2 will receive the following documentation:

- IBM Content Manager for Multiplatforms Planning and Installing Your Content Management System, Version 8, Release 2, September 2004

- IBM Content Manager for Multiplatforms System Administration Guide, Version 8, Release 2, September 2004

7 IT Product Testing

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

7.1 Developer Testing

IBM's approach to security testing for IBM Content Manager for Multiplatforms v8.2 is security functional requirement based. Essentially, IBM developed a set of test cases that correspond to a security functional requirement. Each test case is subdivided into security functions and each test procedure targets the specific security behavior associated with that security function. The test procedures are designed to be exercised manually using the subsystem interfaces.

Test depth is addressed by analyzing the functionalities addressed in the high-level design and associating test cases that cover the addressed functionalities. The high-level design addressed the general functions of the TOE components. Each security function maps the appropriate test cases and the rationale demonstrates why the test cases cover that particular security function.

The developer's *Security Related Test Cases* document includes the configurations for all the platforms claimed along with tests attributed to all the security functions and security-relevant interfaces identified.

The developer tested all claimed platforms and provided actual test results for each of the claimed platforms. The actual results were included in several Excel documents that contain the output log for each applicable test. The output log was a step-by-step representation of the test case results. The spreadsheets correspond to a specific operating system. Each test case result is identified by the test case number and includes the procedures and/or steps and the expected results.

SAIC and the developer consider the detailed test configuration to be proprietary information. However, the Evaluation Team has included a description of the vendor's test configurations in the ETR, Part 2.

The evaluation team analyzed the vendor test procedures to ensure adequate coverage and to determine if the interfaces between subsystems were behaving as expected.

The Evaluation Team determined that the developer's actual test results matched the vendor's expected results.

7.2 Evaluation Team Independent Testing

The evaluation team performed testing at the developer site. The evaluation team installed the TOE and ran all of the vendor test procedures on the TOE in the evaluated configuration. The vendor provided a complete set of test results for analysis.

Some issues were noted during the set up and testing. Updates to the vendor documentation have corrected the cause of these issues.

The Evaluation Team exercised the entire set of the vendor's test procedures per the evaluated configuration as described in the IBM DB2® Content Manager for Multiplatforms v8.2 Security Related Test Cases document. This ensured that the Evaluation Team adequately addressed all security functions. The Evaluation Team used the developer's test configurations to perform the tests.

In addition, the Evaluation Team also tested the installation, generation, and start-up procedures for the specific platforms; AIX, Linux, and Windows, to determine, in accordance with ADO_IGS.1.2E, that those procedures result in a secure configuration.

7.3 Evaluation Team Penetration Testing

For its penetration tests, the Evaluation Team focused on the vendor's vulnerability analysis to identify penetration test cases. The Evaluation Team used the developer's test configuration to successfully perform its penetration tests.

8 Evaluated Configuration

The following hardware was used to create the test configurations:

Windows

- IBM PC (Intel Pentium 800 MHz processor or equivalent), CD-ROM reader (for installation)
- 256 MB RAM or greater
- Typical storage requirements are as follows:
    - Minimum of 100 megabytes (MB) of disk space for Server installation and data storage
    - Minimum of 128 MB for each Library Server.
    - Minimum of 512 MB for each resource manager
    - Minimum of 35 MB for System Administration client
    - Minimum of 64 MB for client for Windows
- SVGA display (800 x 600 resolution and 256 color mode)
- Network adapter card

AIX

- RS/6000 based processor, CD-ROM reader (for installation)
- Typical storage requirements are as follows:

    - Minimum of 100 megabytes (MB) of disk space for Server installation and data storage
    - Minimum of 256 MB for each Library Server.
    - Minimum of 512 MB for each resource manager
- SVGA display (800 x 600 resolution and 256 color mode)
- Network adapter card

Linux

- IBM PC (Intel Pentium 800 MHz processor or equivalent), CD-ROM reader (for installation)
- Typical storage requirements are as follows:
    - Minimum of 100 megabytes (MB) of disk space for Server installation and data storage
    - Minimum of 128 MB for each Library Server.
    - Minimum of 512 MB for each resource manager
- SVGA display (800 x 600 resolution and 256 color mode)
- Network adapter card

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

OS	CM + fix packs	DB2 + fix packs	Websphere Application Server	C++ Compiler on Library Server machine
Windows 2000	CM 8.2 FP6	UDB and SDK v8.1 FP4a	5.0.2	Microsoft Visual C++ compiler
AIX 5.1	CM 8.2 FP6	UDB and SDK v8.1 FP4a	5.0.2	IBM VisualAge C++ Professional Batch compiler 6
Linux SUSE 8	CM 8.2	UDB and SDK v8.1 FP5	5.0.2	

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

OS	CM + fix packs
Windows 2000	Content Manager Client for Windows CM 8.2 FP6
Windows XP	Content Manager System Administration Client CM 8.2 FP6

All software items are described in the IBM Content Manager for Multiplatforms Planning and Installing Your Content Management System.

9 Results of the Evaluation

The Evaluation Team conducted the evaluation based on the Common Criteria (CC) Version 2.1 and the Common Evaluation Methodology (CEM) Version 1.0 and all applicable National and International Interpretations in effect.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 3 augmented with ALC_FLR assurance components. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

> "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."

The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report for IBM DB2 ® Content Manager Multiplatform v8.2 Part 2, dated 22 November 2004" which is considered proprietary.

Section 6.2, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> "The verdicts for each CEM work unit in the ETR sections included in Section 15 are each "PASS". Therefore, when configured according to the following guidance documentation:
>
> - IBM DB2® Content Manager for Multiplatforms Planning and Installing Your Content Management System Version 8 Release 2, September 2004, and
>
> - IBM DB2® Content Manager for Multiplatforms System Administration Guide Version 8 Release 2, September 2004
>
> The IBM DB2® Content Manager for Multiplatforms V8.2 TOE (see product identification below) satisfies the IBM DB2® Content Manager Security Target, Version 1.0, 22 November 2004. "

The validation team followed the procedures outlined in the Common Criteria Evaluation and Validation Scheme (CCEVS) publication number 3 for Technical Oversight and Validation Procedures. The validation team has observed the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validation team therefore concludes that the evaluation and its results of pass are complete.

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 a subset of the vendor test suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10 Validator Comments/Recommendations

The validator had no recommendations concerning the TOE.

The IBM DB2® Content Manager Multiplatforms V8.2 makes a claim that the TOE can be supported on multiple Operating System Platforms. However, the evaluation team did not test the full set of operating systems claimed in the ST. The evaluation team did test at least one operating system platforms of each unique type to confirm the vendor's claims of all security functionality. Therefore, the evaluation team concluded that the test configurations were a representative sample of the list included in the ST.

The IBM DB2® Content Manager Multiplatforms V8.2 is not limited to the structured data kept in various databases and backend systems. However, the evaluation team only performed the evaluation testing with the IBM DB2® database and simple test file documents. The evaluation team did test all security functionality using the IBM DB2® database. Therefore, the evaluation team concluded that the evaluation tests demonstrate the claims in the ST are met.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as IBM DB2® Content Manager for Multiplatforms V8.2 Security Target, Version 1.0, 22 November 2004.

The document identifies the security functional requirements necessary to implement Information Flow Protection and TOE Self Protection security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 3 augmented with ALC_FLR.1.

13 Glossary

The following definitions are used throughout this document:

Authorised User: A user who may, in accordance with the TSP, perform an operation

Connectors: Object-oriented programming class that provides standard access to APIs native to specific content servers

Event log: An audit record in the event tables

Privilege set: A group of privileges that can be assigned to a user

Password: A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Resource: Any data entity that is stored on a resource manager in digital form. Objects can include, but are not limited to, JPEG images, MP3 audio, AVI video, or a plain text file. For example, a few of the formats that are supported natively by Content Manager are: Microsoft Word, Lotus® WordPro, TIFF, and JPEG

Software: The programs and associated data that can be dynamically written and modified.

Target of Evaluation (TOE); An information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

User Group: A group of individual users who perform similar tasks

14 Abbreviations

Abbreviations	Long Form
ACL	Access Control List
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CEM	Common Evaluation Methodology
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IATF	Information Assurance Technical Framework
IT	Information Technology
ITSEC	IT Security Evaluation Criteria
I&A	Identification and Authentication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OR	Observation Report
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
QA	Quality Assurance
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
TTAP/CCEVS	Trusted Technology Assessment Program / Common Criteria Evaluation and Validation Scheme

15 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, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Evaluation Technical Report for IBM DB2® Content Manager for Multiplatforms V8.2 Part 2.

[8] IBM DB2® Content Manager Security Target, Version 1.0, 22 November 2004.

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