National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme
Validation Report

Xacta IA Manager™ Enterprise Edition V4.0 SP2, Build 485

Report Number: CCEVS-VR-05-0085
Dated: January 14, 2005
Version: 1.0

ACKNOWLEDGEMENTS

Validation Team

Rashida F. Doss
Lead Validator
National Security Agency
Fort Meade, MD 20755-6740

Timothy J. Bergendahl
Validator
The MITRE Corporation
Bedford, MA 01730-1420

Common Criteria Testing Laboratory

CygnaCom Solutions
Suite 5200
7925 Jones Branch Drive
McLean, VA 22102-3321

Evaluation Team

Herbert Markle

TABLE OF CONTENTS

1   Executive Summary

This Validation Report (VR) documents the NIAP Validators' assessment of the CCEVS evaluation of Xacta IA Manager^{TM} Enterprise Edition V4.0 SP2, Build 485 (hereafter Xacta IA Manager). A product of Xacta® Corporation, Ashburn, VA, Xacta IA Manager is an information security risk management application. The evaluation of Xacta IA Manager at EAL2 was performed by the CygnaCom Solutions Common Criteria Testing Laboratory (CCTL), McLean, VA beginning on February 19, 2004 and completed on January 14, 2005. The evaluation results identified in this validation report (VR) were drawn from the Xacta IA Manager Evaluation Technical Report (ETR) prepared by the CygnaCom CCTL. The Target of Evaluation (TOE) was evaluated using the *Common Criteria for Information Technology Security Evaluation*, Version 2.2, January 2004 [CCV2.2], and the *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Evaluation Methodology, January 2004 [CEMV2.2]. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) best practices as described within CCEVS Publication #3 [CCEVS3] and Publication #4 [CCEVS4]. The Security Target (ST) for Xacta IA Manager is contained within the document *Xacta IA Manager^{TM} Enterprise Edition V4.0 SP2, Build 485 Security Target V1.15*, December 8, 2004 [STV1.15]. The ST has been shown to be compliant with the *Specification of Security Targets* requirements found within Annex A of Part 1 of [CCV2.2]. The CygnaCom Solutions CCTL Evaluation Team concluded that the TOE was found to be Part 2 extended and Part 3 conformant, and recommended that an EAL2 certificate rating be issued for the TOE.

The all-software TOE consists of the Xacta IA Manager that includes the Application Server, Detect Server, Publishing Server, and Graphical User Interface (GUI), all running on the same physical machine. Not part of the TOE, but installed on the same physical machine as the TOE components, are Windows 2000 Server; Internet Explorer 6.0; and Web Services GUI, a JSP/Servlet application that executes via a Tomcat 4.0.6 servlet engine; Oracle 9i server/8i client (for data management); JRE, version j2sdk1.4.2; Microsoft Office 2000 (Microsoft Word and Excel); and Acrobat Reader.

Aspects of the following security functions are controlled/provided by the TOE:
- Security audit
- User data protection
- Identification and authentication
- Security management
- TOE access

The overall Strength of Function (SOF) claim for the TOE is SOF-basic.

The TOE does not claim conformance to any protection profile.

This Validation Report is not an endorsement of Xacta IA Manager by any agency of the United States Government, and no warranty of the product is either expressed or implied.

All copyrights and trademarks are acknowledged.

2 Identification

TOE: Xacta IA Manager^{TM} Enterprise Edition V4.0 SP2, Build 485

Evaluated Software: Xacta IA Manager^{TM} Enterprise Edition V4.0 SP2, Build 485

Developer: Xacta® Corporation
                19886 Ashburn Road
                Ashburn, VA 20147

CCTL: CygnaCom Solutions
                Suite 5200
                7625 Jones Branch Drive
                McLean, VA 22102-3321

CC Identification: *Common Criteria for Information Technology Security Evaluation*,
                Version 2.2, January 2004 [CCV2.2].

Interpretations: There are no applicable interpretations.

CEM Identification: *Common Methodology for Information Technology Security Evaluation*, Version 2.2, Evaluation Methodology, January 2004 [CEMV2.2].

3 Security Policy

The Xacta IA Manager security policy is reflected in the TOE security functional requirements described in Section 5.2 of the ST [STV1.15]. A description of these security policies is as follows.

- The TOE supports four roles, built-in master administrator; administrator; executive; and user. See **FMT_SMR.1 Security roles**, within section 5.2.4 of the ST [STV1.15], for additional details.

- Users of the TOE are required to be identified and authenticated before being allowed access to the system. Table 5-4 within the ST [STV1.15] identifies the password policy rules.

- The TOE provides access control between subjects and objects that is separate from the access controls of the underlying operating system.Table 5-3 within the ST [STV1.15] provides details about the Xacta IA Manager access control policy.

- The TOE provides security management through the use of an administrator interface. A list of security attributes that can be managed by the TOE are identified within Table 5-5 of the ST [STV1.15].

- The TOE provides its own auditing capabilities. Auditable events include start-up and shutdown of the audit functions, as well as the events identified within Table 5-2 of the ST [STV1.15].

- The TOE causes an access banner to be displayed regarding unauthorized use of the TOE prior to the establishment of a user session. See **FTA_TAB.1 Default TOE access banners**, within Section 5.2.6 of the ST [STV1.15], for additional details.

4   Assumptions and Clarification of Scope

4.1   Usage Assumptions

For secure usage, the operational environment must be managed in accordance with the documentation associated with the following EAL2 assurance requirements.

ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance

4.2   Environmental Assumptions

The environmental assumptions listed in the following table are required to ensure the security of the TOE.

Environmental Assumptions

Assumption	Description
A.Access	It is assumed that only authorized TOE, database, and operating system administrators have access to the data stored in the database and the underlying operating system.
A.Admin	The administrator is trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.
A.Intranet	It is assumed that the Xacta IA Manager Enterprise Edition Server is

Assumption	Description
	deployed on a trusted intranet.
A.Manage	It is assumed that one or more authorised administrators are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the Xacta IA Manager Enterprise Edition Server host.
A.Physical	The TOE components critical to the security policy enforcement will be protected from unauthorized physical modification.
A.Time	It is assumed that the underlying operating system provides reliable time stamps.
A.Users	It is assumed that users will protect their authentication data.

4.3 Clarification of Scope

The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product. Applicable threats are shown in the following table.

Threats

Threat	Description
T.Abuse	An undetected compromise of the TOE may occur as a result of an authorised user of the TOE (intentionally or otherwise) performing actions the individual is authorised to perform.
T.Access	An authorised user of the TOE may access information or resources without having permission from the person who owns, or is responsible for, the information or resource.
T.BadPassword	Users may not select good passwords on their own, allowing attackers to guess their passwords and obtain unauthorised access to the TOE.
T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorised access to TSF.
T.Mismanage	Authorised administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorised access to resources protected by the TOE.
T.Privil	An unauthorised user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.Tamper	An attacker may attempt to modify TSF programs and data.
T.Transmit	TSF data may be disclosed or modified by an attacker while being transmitted between the TOE and its users.
T.Undetect	Attempts by an attacker to violate the security policy may go

Threat	Description
	undetected. If the attacker is successful, TSF data may be lost or altered.
T.Walkaway	A user may leave his workstation without logging out. A user may leave his workstation without logging out thus allowing unauthorized users to gain access to resources and data protected by the TOE.

5   Architectural Information

Xacta IA Manager TOE is an information security risk management application that consists of the Application Server; Detect Server; Publishing Server; and Graphical User Interface (GUI), as depicted in the following figure.
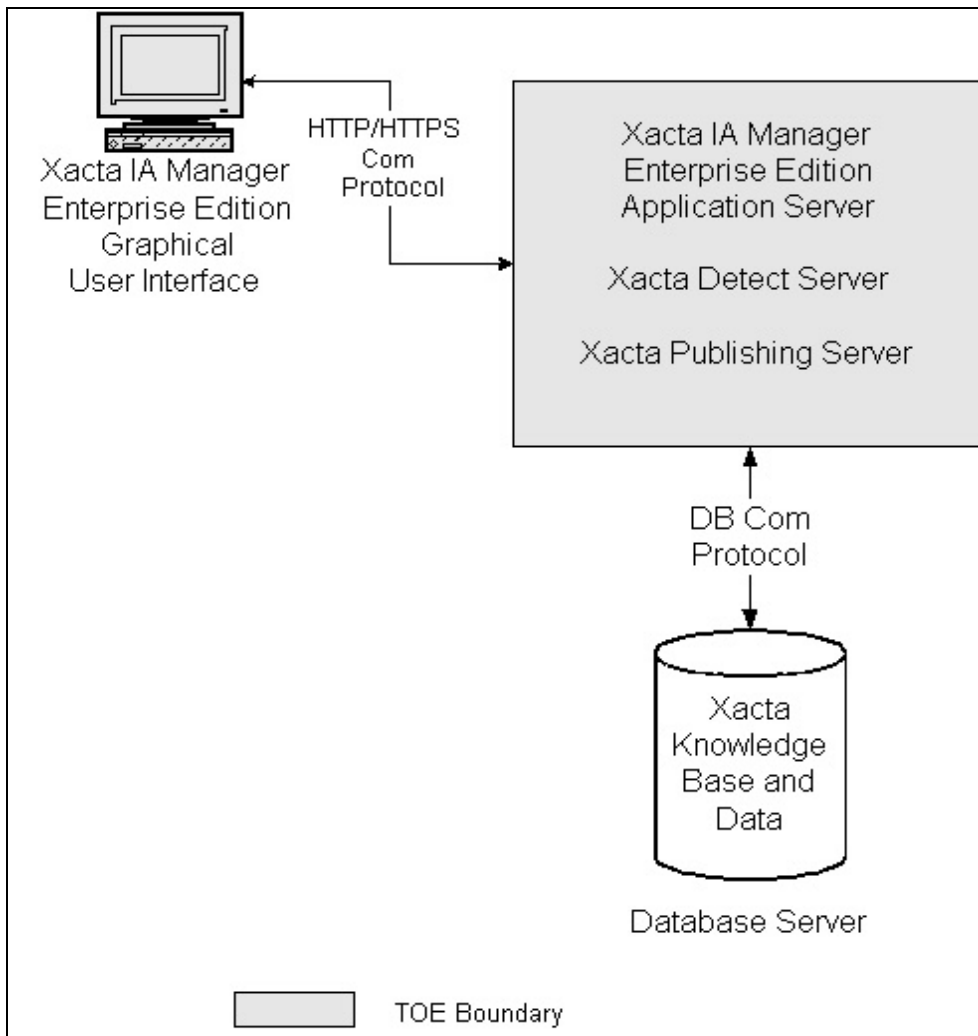
An architectural diagram of the TOE

The Application Server provides the core business logic of the application. As such, all other TOE components communicate with the Application Server. Security functions of the Application Server include:

- Identification;
- Authentication;
- Access Control;
- Authorization;
- Audit.

The Detect Server is a Java-based scanning utility that utilizes standard network technologies. Capabilities of the Detect Server include:

- Discovery scanning;
- Vulnerability scanning;
- Collection of data obtained from host agents.

The Publishing Server produces the files associated with Certification and Accreditation efforts in Adobe PDF or Microsoft Word format.

All security functions of the TOE are managed via the Xacta IA Manager GUI.

The following software is <u>not</u> part of the TOE, but is installed on the Xacta IA Manager server machine:

- Microsoft Windows 2000 Server;
- Internet Explorer 6.0;
- Web services GUI, a JSP/Servlet application that is executed with Tomcat 4.0.6;
- Oracle 9i server/8i client (for data management);
- Java Runtime Environment (JRE), j2sdk.1.4.2;
- Microsoft Office 2000 (Microsoft Word and Microsoft Excel);
- Acrobat Reader.

6 Documentation

The following table is a list of the evaluation evidence used to support this evaluation.

Assurance Measure	Document Title and Date
Security Target	*Xacta IA Manager Enterprise Edition V4.0 SP2 Security Target V1.15*, December 8, 2004
CM Documentation	*Configuration Items for Xacta IA Manager Enterprise Edition Version 4.0 SP2*, 01 December 2004

Delivery Procedures	*Delivery Procedures for Xacta IA Manager Enterprise Edition Version 4.0 SP2*, 26 September 2004
Installation, Generation, and Start-Up procedures	*Secure Installation & Configuration Supplement for Xacta IA Manager Enterprise Edition Version 4.0 SP2*, 03 November 2004
Functional Specification	*Security Functional Specification for Xacta IA Manager Enterprise Edition Version 4.0 SP2*, 09 November 2004
	Xacta IA Manager Enterprise Edition Reference Manual, 24 September 2004
High-Level Design	*High Level Design for Xacta IA Manager Enterprise Edition Version 4.0 SP2*, 21 August 2004
	Xacta IA Manager Enterprise Edition Reference Manual, 24 September 2004
Representation Correspondence	*Informal Correspondence Demonstration for Xacta IA Manager Enterprise Edition Version 4.0 SP2*, 21 August 2004
Administrator Guidance	*Xacta IA Manager Enterprise Edition Reference Manual*, 24 September 2004
User Guidance	*Xacta IA Manager Enterprise Edition Reference Manual*, 24 September 2004
Test Coverage Analysis	*Test Coverage Analysis for Xacta IA Manager Enterprise Edition Version 4.0 SP2*, 11 August 2004
Test Documentation	*Security Test Plan for Xacta IA Manager Enterprise Edition Version 4.0 SP2*, 26 September 2004
TOE for Testing	*Xacta IA Manager –Enterprise Edition V4.0 SP2 build 485*
SOF Analysis	*Strength of Function Analysis for Xacta IA Manager Enterprise Edition Version 4.0 SP2*, 11 August 2004
Vulnerability Analysis	*Vendor Vulnerability Analysis for Xacta IA Manager Enterprise Edition Version 4.0 SP2*, 07 October 2004

7   IT Product Testing

The CygnaCom Solutions CCTL provided tests procedures and test results applicable to the Xacta IA Manager (for TOE testing) as well as for the TOE and its environment (for

vulnerability testing). Testing was conducted on 20-21 October 2004 at Xacta Corporation, Ashburn, VA.

Prior to testing, the developer prepared functional test procedures that were based on the security functional requirements listed in Table 6-1 of the ST [STV1.15]. The approach was to identify each component that could be proven through the applicable TOE Security Functions Interface (TSFI), then prepare individual tests.

During TOE testing, the Evaluation Team executed the developer's test procedures, as well as additional tests designed by the Evaluation Team. Product vulnerability testing was also conducted by the Evaluation Team.

Test results, which are contained in proprietary reports, were satisfactory to both the Evaluation Team and the Validation Team.

8   Evaluated Configuration

The evaluated configuration was on a single server deployment that included the following:

- Xacta IA Manager Publishing, Application, and Detect Servers running on the same physical machine operating with Windows 2000 Server. This machine also hosts the web services GUI engine. Oracle is also installed on this physical machine for data management.

- The Xacta IA Manager Graphical User Interface was presented on both a separate machine running Internet Explorer on a Windows 2000 workstation and from the Windows 2000 server described above.

In addition, the Xacta IA Manager was configured so that the built-in Master Administrator account's remote login capability was disabled. The TOE included the Xacta IA Manager Publishing, Application, and Detect Server software, including the Xacta IA Manager Graphical User Interface.

9   Results of the Evaluation

The Xacta IA Manager satisfies the EAL2 security assurance requirements identified in Part 3 of the *Common Criteria* [CCV2.2]. These requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

The CygnaCom CCTL Evaluation Team followed the procedures outlined in CCEVS Scheme Publication #4, *Guidance to Common Criteria Testing Laboratories* [CCEVS4].

The Evaluation Team concluded that the TOE was CC Part 2 extended and CC Part 3 conformant, and recommended that an EAL2 certificate rating be issued for the TOE.

The Validation Team agreed with the conclusion of the CygnaCom CCTL Evaluation Team that an EAL2 certificate rating be issued for Xacta IA Manager^{TM} Enterprise Edition V4.0 SP2, Build 485.

10 Validator Comments/Recommendations

- As an all-software TOE, consumers must be aware that the underlying operating system and the hardware platform upon which the operating system is installed provide the security upon which the TOE relies. Neither the underlying operating system nor the hardware platform was a component of this evaluation.

- **FTA_TAB.1 Default TOE access banners** provides a very useful feature since such banners are frequently required before a system is allowed to process certain kinds of information.

- Both Xacta Corporation and the CygnaCom Solutions CCTL worked closely and openly with the Validators during this evaluation.

11 Security Target

The Security Target for Xacta IA Manager is contained within the document
Xacta IA Manager^{TM} Enterprise Edition V4.0 SP2 Security Target V1.15, December 8,
2004 [STV1.15]. The ST is compliant with the *Specification of Security Targets*
requirements found within Annex A of Part 1 of the CC [CCV2.2].

12 Glossary

The following table is a glossary of terms used within this validation report.

Acronym	Expansion
CC	*Common Criteria for Information Technology Security Evaluation*. [Note: Within this Validation Report, CC always means Version 2.1, dated August 1999.]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CCIMB	Common Criteria Interpretations Management Board
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
I&A	Identification and Authentication
JRE	Java Runtime Environment
JSP	Java Server Page
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

13 Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap.nist.gov/cc-scheme).

- CygnaCom Solutions (http://www.cygnacom.com).

- Xacta® Corporation (http://www.xacta.com).

CCEVS Documents

[CCV2.1] *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999.

[CEMV1.0P2] *Common Methodology for Information Technology Security Evaluation*, Version 1.0, Part 2: Evaluation Methodology, August 1999.

[CCEVS3] *Guidance to Validators of IT Security Evaluations*, Version 1.0, February 2000.

[CCEVS4] *Guidance to Common Criteria Testing Laboratories*, Draft, Version 1.0, March 2000.

Other Documents

[STV1.15] *Xacta IA Manager^{TM} Enterprise Edition V4.0 SP2 Security Target V1.15*, December 8, 2004.