National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Siebel eBusiness Platform Version 7.8.2

Report Number: CCEVS-VR-06-0003
Dated: January 30, 2006
Version: 1.0

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

Table of Contents

Table of figures

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the Siebel eBusiness Platform Version 7.8.2, a product of Siebel Systems Inc, San Mateo, CA.

This VR is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Siebel eBusiness Platform is an application platform which provides a complete suite of configuration and operational tools and services including interfaces, data synchronization and replication, workflow, assignment, and security. The application platform masks the underlying specificity of the development environment, specifically the Operating System (OS) and the Database Management System (DBMS) enabling the development of applications that are independent of the hardware and OS platforms and of the programming language. Siebel eBusiness Applications are developed and deployed atop the Siebel eBusiness Platform. The Target of Evaluation (TOE) consists of the graphical user interface (GUI) and the Siebel Application Server (SAS) components. All user operations and security management functions are performed via the GUI. The SAS component runs on a server host and provides the core business logic of the application.

Aspects of the following security functions are controlled / provided by the TOE in conjunction with its information technology (IT) environment:

- Identification and Authentication
- User data protection
- Security Audit
- Security management
- Confidentiality of network transmissions

The following are explicitly excluded from the TOE configuration, but are included in its IT environment:

- Hardware platforms and Windows 2000 Operating Systems;
- DBMS server (Oracle 9i Enterprise Server);
- Web browser (Microsoft Internet Explorer);
- Web server (Microsoft Internet Information Services);
- Cryptographic services of the operating system supporting HTTPS; and
- Network hardware and software (e.g., firewalls and routers)

The evaluated configuration is the Siebel eBusiness Platform Application Server V7.8.2 (with the Strong Encryption Pack option) running on Microsoft Windows 2000 SP4 Server.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed during December 2005. The information in this report is

derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the CygnaCom CCTL. The evaluation team determined that the product is Common Criteria version 2.2 [CCV2.2] Part 2 and Part 3 conformant, and meets the assurance requirements of EAL2 from the Common Methodology for Information Technology Security Evaluation, Version 2.2, Part 2: Evaluation Methodology [CEMV2.2]. The product is not conformant with any published Protection Profiles, but rather is targeted to satisfying specific security objectives while countering specific threats.

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 Siebel eBusiness Platform is contained within the document Security Target for Siebel eBusiness Platform Version 2.0 [ST]. The ST has been shown to be compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of CC.

2. Identification

Target of Evaluation:	Siebel eBusiness Platform V7.8.2
Evaluated Software:	Siebel eBusiness Platform V7.8.2
Developer:	Siebel Systems, Inc. San Mateo, CA
CCTL:	CygnaCom Solutions Suite 100 West 7925 Jones Branch Drive McLean, VA 22102-3305
Validation Team:	Yi-Fang Koh (The MITRE Corporation) Sunil Trivedi (The MITRE Corporation)
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 2.2, Rev 256
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 2.2, Part 2: Evaluation Methodology
Interpretations:	CCIMB-2004-01-001, January 2004.

3. Security Policy

The TOE's security policy is expressed in the security functional requirements identified in the section 5.2 in the ST. A description of the principle security policies is as follows:

- **Identification and authentication**

The TOE in conjunction with the IT environment requires users to be identified and authenticated before being allowed access to the system. The user login information entered via the TOE's GUI is sent by the SAS component to a Lightweight Directory Access Protocol (LDAP) Server to check the validity of the username and password.

- **User data protection**

The TOE restricts access to data records stored in its underlying database. The TOE provides two access control mechanisms:

- **View**: Access to each database table, or "View" in Siebel terminology, is restricted to individual users by the administrator. The administrator organizes "Views" into named lists, or "responsibilities" in Siebel terminology. The TOE only displays and permits access to the "Views" that are associated with the user's "responsibilities".
- **Record**: Access to a data record within a table may be further restricted to the record's owner by the administrator. The TOE supports several abstractions of the user's identity or group memberships (i.e., "organizations", "divisions", "positions", and "access groups" in Siebel terminology) to determine an ownership match.

- **Security audit**

The TOE is capable of generating audit records**.** The GUI provides a capability for searching, sorting, and viewing audit records.

- **Security management**

The TOE's GUI provides an interface for the administrator to manage the TOE security functions.

A summary of the SFRs for the TOE and IT environment are included in the tables below. In these following tables, "*" refers to all iterations of a component.

TOE Security Functional Requirements

Class FAU: Security Audit	
FAU_GEN.1	Audit data generation
FAU_GEN.2	User identity association
FAU_SAR.1	Audit Review
FAU_SAR.2	Restricted Audit Review
FAU_SAR.3	Selectable Audit Review
FAU_SEL.1	Selective audit
Class FDP: User Data Protection	
FDP_ACC.2	Complete access control
FDP_ACF.1	Security attribute based access control

Class FIA: Identification & Authentication	
FIA_ATD.1	User attribute definition
FIA_UAU.7	Protected authentication feedback
FIA_USB.1	User-subject binding
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behavior
FMT_MSA.1*	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
Class FPT: Protection of the TSF	
FPT_RVM_EXP.1-1	Non-bypassability of the TSP
FPT_SEP_EXP.1-1	TSF domain separation

IT Environment Security Functional Requirements

Class FCS: Cryptographic Operation	
FCS_CKM.1*	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1*	Cryptographic operation
Class FIA: Identification & Authentication	
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
Class FMT: Security Management	
FMT_MSA.2	Secure security attributes
Class FPT: Protection of the TSF	
FPT_RVM_EXP.1-2	Non-bypassability of the TSP
FPT_SEP_EXP.1-2	TSF domain separation: Operating System
FPT_STM.1	Reliable time stamps
FPT_ITC.1	Inter-TSF confidentiality during transmission

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

- It is assumed that TOE components are stored in a secure physical location to prevent unauthorized physical modification.
- Only trusted, knowledgeable, and authorized administrators will be able to manage, configure, operate, and access TOE, database and the underlying operating system according to the TOE documentation.
- No untrusted users will access the TOE or no untrusted software or data will reside on the TOE.
- TOE depends on the underlying operating system for a reliable time stamps.
- It is assumed that users will protect their authentication data.
- It is assumed that there is the capability to hash and store user passwords.

4.3 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:
1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL2 in this case).
2. This evaluation only covers the specific version identified in this document, and not any later versions released or in process.
3. As with all EAL2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" (as this term is defined in the CC and CEM) or "vulnerabilities" to objectives not claimed in the ST.

The ST provides additional information on the assumptions made and the threats countered.

5. Architectural Information

The Siebel eBusiness Platform consists of the Siebel Application Server, the Database Server, the LDAP Directory Server and the Graphical User Interface. The TOE Components only includes the Siebel Application Server and Graphical User Interface.

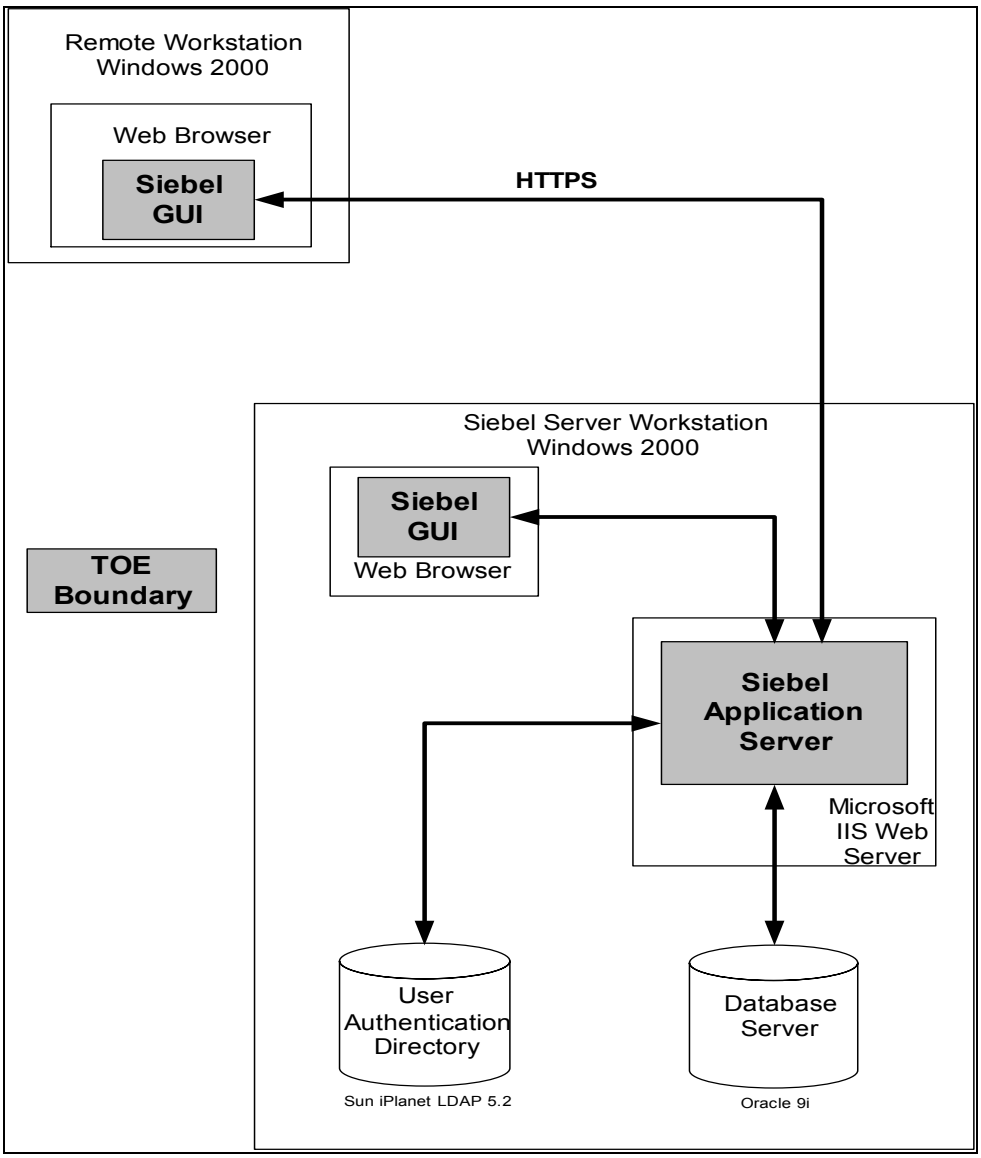

Figure 1. TOE Physical Boundary.

6. Documentation

The following is a list of the end-user documentation that was used to support this evaluation:

- Siebel eBusiness Platform V7.8.2 Security Target V2.0, dated November 9, 2005
- Applications Administration Guide v7.8, Rev A, dated June 2005
- Security Guide for Siebel Business Applications v7.8, Rev A, dated May 2005
- Siebel Systems Administration Guide v7.8, dated February 2005
- Siebel Release Notes V7.8
- Maintenance Release Guide Version 7.8.2

7. IT Product Testing

7.1 Developer Testing

The vendor testing covered the security functions identified in Section 6.1 of the ST. These security functions were: Security audit, Manage User Access, User Login, and Security Management. At EAL2, vendor testing must demonstrate correspondence between the tests and the functional specification. However complete testing is not required; "coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the TOE Security Function (TSF) have been tested."(CEM 6.8.2.2).

The testing was focused on demonstrating that the SFRs worked as claimed in the ST. The test procedures consisted primarily of manually invoking functions described in the product's user and administrative guides and verifying the function's behavior. In general, only those user interface functions that were directly related to SFRs were explicitly verified.

The evaluator determined that the vendor tested (at a high level) most of the security-relevant aspects of the product that were claimed in the ST. The evaluator determined that the developer's tests were sound in their approach. The test document provided the configuration of the test hardware and software, the objective for each of the tests, and test procedures. The information provided was adequate to be able to reproduce the tests. The evaluators determined that the developer's approach to testing the TSFs was appropriate for this EAL2 evaluation.

7.2 Evaluator Independent Testing

At EAL2, the stated purpose of the evaluator's independent testing activity "is to determine, by independently testing a subset of the TSF, whether the TOE behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests." (CEM 6.8.4.1). As a result, the testing at EA2 may not be systematic and the end-users should not assume that all claims in the ST have been explicitly verified by either the developer or the evaluators.

The installation of the TOE was done in accordance with the product's Administrator and Installation guides which specifies the configuration of Microsoft's Windows 2000. The latest security-critical patches for Windows 2000 Professional SP4, Windows 2000 Advanced Server SP4, and Oracle 9i Version 9.2.0.1 were installed prior to the evaluation testing activities

The evaluation team reran all of the developer tests and verified the results. The evaluation team then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

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

7.3 Strength of Function

The TOE depends on the strength of the passwords used to authenticate access to the SAS. For authentication mechanisms a qualification of the security behavior can be made using the results of a quantitative or statistical analysis of the effort required to overcome the mechanism. While the TOE includes a strength-of-function (SOF) claim of SOF-basic, which effectively requires resistance to password guessing attacks of greater than one day, an SOF analysis was not required because the authentication requirements (i.e., FIA_UAU.2) are delegated to the IT environment. The Sun iPlanet LDAP 5.2 server provided the authentication mechanism during testing.

7.4 Vulnerability Analysis

The developer searched for publicly known vulnerabilities specifically related to the TOE. No publicly-known vulnerabilities specific to the evaluated version of Siebel eBusiness Platform were found. The following public domain sources were used to identify and search for relevant vulnerabilities:

- http://cve.mitre.org/cve
- http://www.securityfocus.com
- http://www.siebel.com
- http;//www.google.com

Known vulnerabilities in the IT environment could also be exploited to bypass the TOE's security policies. While these vulnerabilities are outside the scope of the evaluation, it is expected that the customer will installed the latest security critical patches to the operating system and database software. Under unusual circumstances a patch to TOE may also be required to address compatibility issues with a specific operating system or database patch. The customer is advised check the Siebel support web site for any restrictions on specific patches to components of the IT environment.

The assumed level of expertise of an attacker is unsophisticated, with access to only standard equipment and public information about the product. The specific threats that the TOE is designed to counter are listed in section 3.2.1 of the ST.

8. Evaluated Configuration

The evaluated version of the Siebel eBusiness Platform is version 7.8.2. Siebel provides delivery of this product's components through the Siebel FTP server. It requires authentication information (user name and password) prior to allowing access to the file

containing the TOE. Authentication data is provided to customers via email or verbally. The authentication data is good for one-time file transfer of the TOE.

9. Results of Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 2.2 of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of issues requiring resolution or clarification within the evaluation evidence. 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.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL. The security assurance requirements are displayed in the following table.

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ACM_CAP.2	CM Documentation
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Functional specification
ADV_HLD.1	High-level design
ADV_RCR.1	Representation Correspondence
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Test Coverage Analysis
ATE_FUN.1	Test Documentation
ATE_IND.2	Independent testing
AVA_SOF.1	Strength of TOE Analysis
AVA_VLA.1	Vulnerability analysis

10. Validator Comments/Recommendations

The Validation Team agreed with the conclusion of the CygnaCom CCTL Evaluation Team, and recommended to CCEVS Management that an EAL2 certificate rating be issued for the Siebel eBusiness Platform V7.8.2.

11. Security Target

The Security Target for Siebel eBusiness Platform V7.8.2 is contained within the document Security Target for Siebel eBusiness Platform V7.8.2, Version 2.0 [ST]. The ST is compliant with the Specification of Security Targets requirements found within Annex A of Part 1 of the CC.

12. Glossary

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

Acronym	Expansion
CC	Common Criteria [CCV2.2]
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Criteria Evaluation Methodology [CEMV2.2]
DBMS	Database Management System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OS	Operating System
PP	Protection Profile
SAS	Siebel Application Server
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation

13. Bibliography

URLs

- Common Criteria Evaluation and Validation Scheme (CCEVS): (http://niap.nist.gov/cc-scheme).
- CygnaCom Solutions CCTL (http://www.cygnacom.com).
- Siebel Systems, Inc. (http://www.siebel.com).

CCEVS Documents

- [CCV2.2] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004.
- [CEMV2.2] Common Methodology for Information Technology Security Evaluation, Version 2.2, Part 2: Evaluation Methodology, January 2004.
- [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 2001.

Other Documents

- [ST] Security Target for Siebel eBusiness Platform V7.8.2, Version 2.0, November 9, 2005