National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

DBsign for HTML Applications Version 4.0

Report Number: CCEVS-VR-VID10407-2011
Dated: 9 March 2011
Version: 0.5

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 6940
Fort George G. Meade, MD 20755-6940

Contents

1 Executive Summary

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Gradkell DBsign for HTML Applications version 4.0, the target of evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This report is not an endorsement of the TOE by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation of the Gradkell DBsign for HTML Applications version 4.0 product was performed by DSD Laboratories, Inc., in Bridgeport, WV in the United States of America (USA) and was completed in January, 2010. The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR), DBsign User Guidance as listed in section 7 of this document, and the functional testing report. The ST was written by Saffire Systems. The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 July 2009, Evaluation Assurance Level 2 (EAL 2), and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 r.3, July 2009.

The DBsign product is a software only solution providing a digital signature system that supports cryptographic data integrity and non-repudiation for data stored in relational databases. DBsign supports digital signature operations for data stored within a database and other data provided by the application. A co-existing application can interface to DBsign using DBsign's API to perform digital signature operations for the given application.

DBsign includes the following major components:

- Client-side signing component called the DBsign Universal Web Signer (DBsign UWS)
- Server-side component called the DBsign Server
- DBsign Administration Tools, a set of graphical administration tools used to administer DBsign configuration data

These components work together to support the integration of digital signatures into applications.

The TOE requires the following software components and supports the following network devices:

DBsign Universal Web Signer. The DBsign Universal Web Signer (UWS) is a Java applet and requires a Sun Java 1.5 (or higher) JRE (Java Runtime Environment) to run. The DBsign UWS requires that the hardware and software requirements for both the JRE and the host operating system have been met.

DBsign Server. The DBsign Server is a Java Servlet and requires a Sun Java 1.6 (or higher) JRE (Java Runtime Environment) and a J2EE application server to run. The DBsign Server will run within any J2EE compliant application server supporting the Java Servlet API version 2.2 or higher provided that the hardware and software requirements of the JRE, the J2EE application server and the host operating system have been met.

Administration Tools. The DBsign Administration Tools is a Java GUI application and requires a Sun Java 1.6 (or higher) JRE (Java Runtime Environment) to run. The DBsign Administration Tools require that the hardware and software requirements for both the JRE and the host operating system have been met.

Configuration Editor. The DBsign Configuration Editor is a Java GUI application and requires a Sun Java 1.6 (or higher) JRE (Java Runtime Environment) to run. The DBsign Configuration Editor requires that the hardware and software requirements for both the JRE and the host operating system have been met.

CRL Updater. The DBsign CRL Updater is a Java command line application and requires a Sun Java 1.6 (or higher) JRE (Java Runtime Environment) to run. The DBsign CRL Updater requires that the hardware and software requirements for both the JRE and the host operating system have been met.

2 Identification of the TOE

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	DBsign for HTML Applications version 4.0
Protection Profile	The PP to which this ST conforms is defined in terms of packages. The ST claims conformance to the following Protection Profile (PP): U.S. Government Basic Robustness Public Key-Enabled Applications (PKE) PP with the following packages 1. Certification Path Validation (CPV) – Basic 2. CPV – Basic Policy 3. CPV - Policy Mapping 4. CPV – Name Constraints 5. PKI Signature Generation 6. PKI Signature Verification 7. Online Certificate Status Protocol (OCSP) Client

	8. Certificate Revocation List (CRL) Validation 9. Audit at Basic Robustness Assurance, Version 2.8, May 1, 2007.
Security Target	DBsign for HTML Applications Version 4.0 Security Target Version 1.0
Dates of Evaluation	December 2009 – January 2011
Conformance Result	EAL2 augmented with ALC_FLR.2
Common Criteria Version	Common Criteria for Information Technology Security Evaluation Version 3.1 R3, July 2009
Common Evaluation Methodology (CEM) Version	CEM Version 3.1 R3, July 2009
Evaluation Technical Report	Evaluation Technical Report For DBSign for HTML Applications Version 1.1, February 01, 2011
Sponsor/Developer	Gradkell Inc.
Common Criteria Testing Lab (CCTL)	DSD Information Assurance Laboratory (DIAL)
CCTL Evaluators	Scott Koon (Lead), Chris McNemar
CCEVS Validators	Jean Petty (Lead), Jerome Myers

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all International interpretations with effective dates on or before 19 December 2009.

4 Security Policy

DBsign for HTML Applications version 4.0 provides the following security functions:

- Audit – The DBsign Universal Web Signer, DBsign Server, and the DBsign Administration Tools generate audit records for all audit events associated with digitally signing data and verifying digitally signed data, including requests that fail due to the User Policy.
- User Policy - The TOE provides the optional ability to restrict access to the digital signing operations. By default, the User Policy system is disabled. To support the User

Policy feature, DBsign maintains a list of authorized users and associated certificates, but does not authenticate these users. DBsign relies on the underlying operating system to identify and authenticate the users.

- Security Management - The TOE provides a graphical user interface called the DBsign Administration Tools which implement the security management functionality. The DBsign Administration Tools require that administrators identify and authenticate themselves to the DB in order to connect to the DB and use the selected tools. The DBsign Administration Tools access and store the TOE configuration data in the DB.
- Certification Path Processing - DBsign performs X.509 certification path validation checks. Certification path validation consists of validating certificates starting with the one issued to the subscriber of interest and ending with a trust anchor. DBsign supports X.509 version 3 Certificates. All certification path processing performed by DBsign is X.509 and PKIX RFC3280 compliant. Certificate Revocation Processing - DBsign sends Online Certificate Status Protocol (OCSP) requests in accordance with PKIX RFC 2560 and validates OCSP responses to determine the revocation status of public key certificates. The DBsign administrator configures a list of OCSP responder certificates that are trusted to do OCSP. DBsign establishes trust in the OCSP responder by performing Certification Path Validation. DBsign allows applications to determine the revocation status of a certificate using a Certificate Revocation List (CRL). DBsign may be used to process CRLs obtained from locations indicated by a CRL Distribution Point (CRLDP) extension in a certificate and from the local cache, which is the DBsign certificate and CRL archive. The locations that may be indicated in the CRLDP extension are LDAP or HTTP URLs. DBsign supports X.509 CRLs, version 2.
- PKI Signature Generation – The TOE provides a digital signature function which enables a user to generate a digital signature. The TOE digitally signs data using FIPS validated cryptographic modules in the IT environment. Under normal operations, the client side of DBsign performs the digital signing using the subscriber's certification. Using the Notary Signing feature, the application can request that the DBsign server perform the digital signing using a certificate issued to the application
- PKI Signature Verification – The TOE provides a digital signature function which verifies a digital signature applied to data. This allows for the author of the signed data to be uniquely identified and for the authenticity and integrity of the signed data to be verified. In addition, the digital signature function enforces personal accountability for approved changes made by an administrator to the security sensitive configuration data contained in the DBsign system tables. The TOE verifies digitally signed data and data integrity using FIPS validated cryptographic modules in the IT environment.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The following assumptions are made about the usage of the TOE.

A.Configuration	The TOE will be properly installed and configured.
A.Basic	The attack potential on the TOE is assumed to be "Basic".
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.PHYSICAL	It is assumed that the environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

5.2 Clarification of Scope

DBsign relies upon FIPS 140 validated cryptographic modules in the IT environment to provide all of the cryptographic operations, including digital signature generation and verification.

DBsign accesses the FIPS 140 validated cryptographic modules via PKCS #11 and the Microsoft CryptoAPI. PKCS#11 and the Microsoft CryptoAPI are standardized APIs that provide access to cryptographic modules.

In the evaluated configuration, DBsign must be used with the following FIPS 140-2 validated cryptographic modules that are in the IT environment:

- Windows cryptographic modules accessible via the Microsoft Crypto API that are included with the Windows operating system
- Network Security Services (NSS) Cryptographic Module (software versions 3.2.2 & 3.11.4) accessed via PKCS #11
- Other FIPS 140-2 validated modules accessed via Microsoft CryptoAPI and PKCS #11
- FIPS 140-2 validated modules that execute within a MAC OS X operating system and are accessed via PKCS #11 or Apple Security Framework

In the evaluated configuration, DBsign must be used on the following Common Criteria validated operating systems that are installed and configured in the CC evaluated configuration:

- Microsoft Windows XP Professional and higher (32-bit and 64-bit)
- Microsoft Windows Server 2003 and higher (32-bit and 64-bit) (including Microsoft Windows Server 2008)
- Red Hat Enterprise Linux 5 and higher (32-bit and 64-bit)
- Sun Solaris 8 and higher for SPARC platform (32-bit and 64-bit)
- Sun Solaris 10 and higher for INTEL platform (32-bit and 64-bit)
- Apple Mac OS X 10.6 and higher (32-bit and 64-bit)

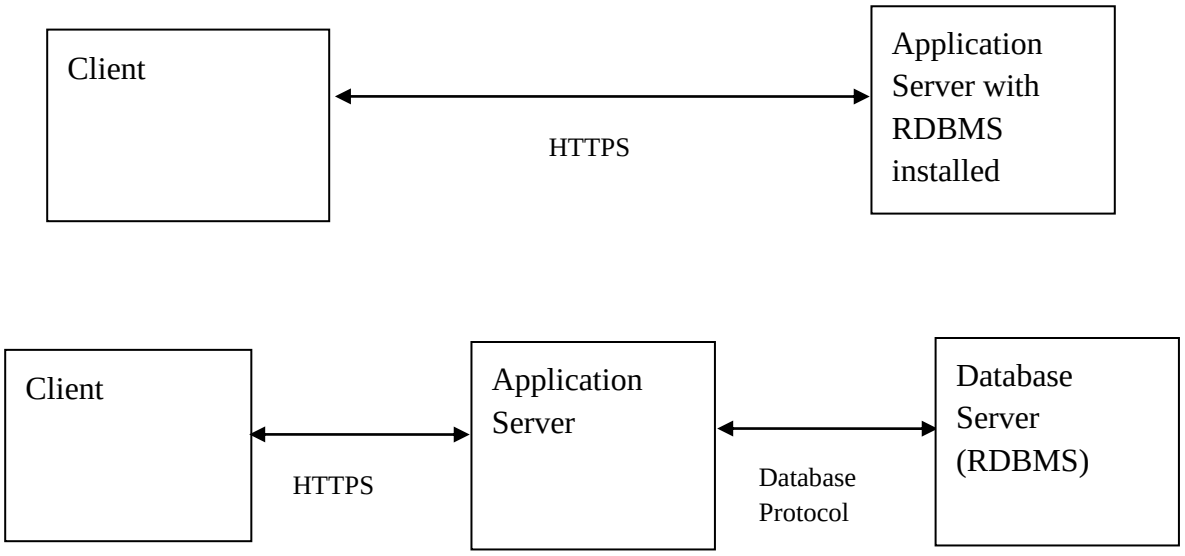
- Oracle Enterprise Linux 5.1 and higher (32-bit and 64-bit)

In addition, the following products must be included on the DBsign platforms:

- Java: Sun JRE 1.5 or higher (32-bit and 64-bit as available)
- Browser:
  - Microsoft Internet Explorer (IE) 6 or higher (32-bit or 64-bit) or
  - Mozilla Firefox 3 and higher (32-bit and 64-bit) or
  - Apple Safari 3 and higher (32-bit and 64-bit)

6 Architectural Information

DBsign is a software only TOE. The client communicates with DBsign Server via the DBsign UWS, an applet downloaded to and executed within their web browser on the client machine. Therefore, the web browser is pointed to the web server hosting DBsign version 4.0 via HTTPS and the web server redirects the query to the application server in which DBsign Server resides. DBsign Server then communicates to a database to retrieve data to be signed by the client via a network protocol recognized by the database (i.e. SQL*Net for Oracle). DBsign can utilize Relational Database Management Systems (RDBMS) products that are accessible through a JDBC driver.



DBsign Configurations

DBsign additionally provides optional security features called the User Policy and Notary Signing features. The User Policy feature provides access control enforcement to digital signatures using templates. The Notary Signing feature provides server-side signing capability.

7 Documentation and Delivery

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the TOE and methodology for delivery of the evaluated configuration.

7.1 Design Documentation

The following guidance documents are delivered to the customer with the product release:

- DBsign Concepts Manual, Version 4.0, Date 11-02-2010
- DBsign for HTML Applications: Integration Manual Version 4.0, Date 11-02-2010
- DBsign for HTML Applications: Installation Manual Version 4.0, Date 11-02-2010
- DBsign Administration Tools Manual Version 4.0, Date 11-02-2010
- DBsign Configuration Editor Manual Version 4.0, Date 11-02-2010
- DBsign for HTML Applications Version 4.0 Release Notes, Date 11-02-2010
- DBsign NIAP Configuration Manual Version 4.0, Date 11-02-102010

All of the above documents were included within the scope of the evaluation.

The following documents were used as evidence but are not delivered to the customer:

- DBsign for HTML Applications Version 4.0 Security Target Version 1.0, Date 01-31-11
- DBsign for HTML Applications version 4.0 Functional Specification Version 0.8, Date 01-03-2011
- DBsign for HTML Applications version 4.0 Security Architecture Document Version 0.3, Date 11-02-2010
- DBsign for HTML Applications version 4.0 TOE Design Version 0.2, Date 01-29-2010
- DBsign for HTML Applications version 4.0 Life-Cycle Document Version 0.5, Date 01-03-2011
- DBsign Test Plan and Procedures Version 0.95, Date 01-03-2011

7.2 Delivery

Gradkell relies upon the physical shipper to maintain the security (integrity) of the TOE while in transit to the customer site. In addition, the customer can confirm the integrity of the TOE by verifying the integrity of the files contained on the CD.

8 IT Product Testing

This section describes the testing efforts of the Developer and the evaluation team.

8.1 Developer Testing

The following test approach was utilized by the vendor in the development of their test methodologies:

- A high-level analysis of the test plan and procedures was performed to determine test coverage. The vendor demonstrated test coverage by showing the mapping between the TSFIs, their corresponding TSFs and Security Functional Requirements and the test cases.
- For each test case, the expected behavior of the interface was tested and the test procedures (test prerequisites, test steps and expected results) were determined by the evaluators to adequately test the interface consistent with the requirements for EAL2.
- The functional specification provided by the vendor provided a mapping of TSFIs to SFRs. Each of the SFRs claimed in the ST was tested at least once and at least 90% the SFR-supporting and SFR-enforcing TSFIs defined in the [FSP] were tested at least once.

8.2 Evaluation Team Independent Testing

The evaluators created a matrix between test cases, TSFI, and SFRs to use while evaluating the vendor testing coverage. This matrix was then used to determine the breadth of testing required to adequately assess the TOE's instantiations of all SFRs and the implementation of all TSFIs. The matrix was used to assess both the completeness of vendor testing, and to ensure that all SFRs were tested by at least one test case. The traceability matrix was found to be consistent with the vendor clams of TSFI and SFRs that were/were not tested by the vendor (all SFRs tested, not all TSFI tested). The TFSI that were not tested will be included in DIAL test cases. The evaluators expanded upon the vendor testing to include all TSFI in order to increase the depth of testing. Although all SFRs and TSFIs are mapped to a vendor or evaluator test case, this is not intended to indicate that the SFRs and TSFIs were completely tested but that one or more aspect was being tested.

Based on analysis from ADV and ATE, the evaluators determined that the vendor and laboratory testing combined are adequate to achieve the level of assurance required for an EAL 2 evaluation.

8.3 Vulnerability Analysis

The evaluators' independent testing included test cases designed to serve as penetration testing. This section further details the thought process in the design of those test cases.

Given the nature of the product as primarily a set of APIs it is difficult to create traditional penetration test cases. This is because the interfaces of the TOE are designed to provide some form of computation and return a result, there is no true access control as it is typically thought of such as in an operating system where the OS is required to make a decision if a user is authorized to access a given piece of data. A user simply having access to the TOE is authorization enough to utilize its API's.

The evaluators opted to conduct cursory vulnerability testing by creating API calls which do not properly conform to the specification. Such as parameters that are invalid, of the wrong data type, and of the wrong size.
Based on analysis from ADV and ATE (elaborated on above), DIAL determined that the combined vendor and laboratory testing are adequate to achieve the level of assurance required for an EAL 2 evaluation.

9 Evaluated Configuration

The TOE was installed and configured following the installation instructions contained in the Gradkell installation and administration guides.

Operating Systems Used in Testing	Microsoft Windows XP Professional Microsoft Windows Server 2003 Microsoft Windows Server 2008 Red Hat Enterprise Linux 5 Sun Solaris 10 Apple Mac OS X
RDBMS Used in Testing	MySQL 5.0 Microsoft SQL Server 2008 R2
Cryptographic Module Used in Testing	Network Security Services (NSS) Cryptographic Module versions 3.12.4 (FIPS 140-2 validation number 1278)
Other Software Requirements	Apache Tomcat 6.0 Java Runtime Environment 6

System Configuration

The operational environment used during testing consisted of various combinations of Application Server, Database Server, and Client virtual machines. The server running the virtual machines is behind a firewall which is connected to the Internet during execution of the Administrator Tools test cases. This is needed because the Administrator Tools test cases require downloading the latest certificates from the DoD website. The IP addresses behind the firewall are not publicly addressable.
The evaluated configuration matched the evaluated configuration set forth by the ST. The operating systems on the Database and Application Server were configured in their respective CC evaluated configurations.

10 Items Excluded from the TOE

There are no items excluded from the TOE.

11 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.
DSD Information Assurance Laboratory has determined that the TOE meets the security criteria in the Security Target, which specifies an assurance level of EAL 2 + ALC_FLR.2. A team of Validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in January 2011.

12 Validator Comments/Recommendations

The TOE was successfully evaluated in the defined evaluated configuration described in section 9 of this Validation Report. The validation team recommends certification of the TOE at EAL 2 augmented with ALC_FLR.2.

13 Security Target

DBsign for HTML Applications Version 4.0 Version 1.0 January 31, 2011

14 Terms

14.1 ST Specific Terminology

DBS	Name of DBsign schema in which the system tables are stored

14.2 Acronyms

API	Application Programming Interface
CC	Common Criteria
DB	Database
EAL2	Evaluation Assurance Level 2
HTTPS	Secure Hyper-Text Transfer Protocol
IT	Information Technology

JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
OSP	Organisational Security Policy
PKI	Public Key Infrastructure
PP	Protection Profile
RDBMS	Relational Database Management Systems
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TOI	Time of Interest
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

15 Bibliography

Common Criteria (CC) for Information Technology Security Evaluation – July, 2009 Version 3.1, Revision 3, CCMB-2006-09-001.

DBsign for HTML Applications Version 4.0 Security Target Version 1.0 January 31, 2011

Evaluation Technical Report For DBSign for HTML Applications Version 1.1, February 01, 2011

VID10407 Test Plan and Test Results For Gradkell, Inc. DBsign for HTML Applications v4.0 Version 1.1, February 01, 2011

U.S. Government Basic Robustness Public Key-Enabled Applications (PKE) PP, Version 2.8, May 1, 2007.