National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Gradkell Systems, Inc.

DBsign for Client/Server Applications Version 3.0

Report Number: CCEVS-VR-05-0127
Dated: 30 September 2005
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

ACKNOWLEDGEMENTS

Validation Team

Patrick W. Mallett, PhD
Roberta J. Medlock
The MITRE Corporation
McLean, VA

Common Criteria Testing Laboratory

SAVVIS Communications
ARCA Common Criteria Testing Laboratory
Sterling, VA

Table of Contents

1 EXECUTIVE SUMMARY

The evaluation of DBsign for Client/Server Applications was performed by the Arca Common Criteria Testing Laboratory (CCTL) in the United States and was completed on 14 September 2005.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (CEM) Version 2.2 for conformance to the Common Criteria for IT Security Evaluation Version 2.2. DBsign for Client/Server Applications (i.e., the TOE) is a digital signature solution that includes a set of APIs that is installed to an IT environment client system.

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 DBsign Data Security Suite 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, 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 Arca CCTL evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 2) have been met.

1.1 Evaluation Details

Evaluated Product:	DBsign for Client/Server Applications Version 3.0
CCTL:	Arca Common Criteria Testing Laboratory
Evaluation Completion:	14 September 2005
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004, CCIMB-2004-01-001, CCIMB-2004-01-002, CCIMB-2004-01-003.

CEM:	Common Evaluation Methodology for Information Technology Security, Version 2.2, January 2004, CCIMB-2004-01-004.
Evaluation Assurance Class:	EAL 2

1.2 Interpretations

The evaluation team determined that the following national (NIAP) interpretations were applicable to this evaluation. No international (CCIMB) interpretations were applicable to this evaluation.

Affected Requirements	Interpretation Number	Description
FDP_ACF.1.3 FDP_ACF.1.4	0407	Empty Selections Or Assignments
FAU_REC.1.2a	0410	Auditing Of Subject Identity For Unsuccessful Logins
FAU_STG.1.2	0422	Clarification Of "Audit Records"

2 OVERVIEW

DBsign for Client/Server Applications is a digital signature product that provides verifiable cryptographic data integrity and non-repudiation for data stored in relational databases. DBsign supports digital signature operations for data stored within a database and application-constructed data stored within memory buffers or files. DBsign performs both digital signature generation and verification.

DBsign is a tool-kit with an application programming interface (API). DBsign APIs provide an interface for co-existing applications. Integration of digital signature functionality can be achieved programmatically through a system of API calls rather than having to integrate the actual source code of DBsign into the co-existing application.

The DBsign APIs in turn use another system of APIs to achieve the cryptographic support functions necessary to performs digital signature generation and verification. The DBsign Crypto Adaptor (DCA) programmatically integrates the cryptographic functionality of the RSA BSAFE Crypto-C API Toolkit version 5.2.1.

DBsign resides on the client machine. DBsign then communicates with a database, running on the server, to retrieve data to be signed by the client via a network protocol recognized by the database (i.e. SQL*Net for Oracle). DBsign supports most Relational Database Management Systems (RDBMS).

3 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;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1 Evaluation Identifiers

Evaluation Scheme:	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluation Completion:	14 September 2005
TOE:	DBsign for Client/Server Applications Version 3.0
PP:	The TOE does not claim conformance to a PP.

ST:	DBsign Data Security Suite, DBsign for Client/Server Applications Version 3.0 Security Target
CC:	Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004, CCIMB-2004-01-001, CCIMB-2004-01-002, CCIMB-2004-01-003.
CEM:	Common Evaluation Methodology for Information Technology Security, Version 2.2, January 2004, CCIMB-2004-01-004.
Developer:	Gradkell Systems, Inc. 4910 University Square, Suite 2 Huntsville, AL., 35816
Evaluation Assurance Class:	EAL 2
CCTL:	SAVVIS Communications Arca Common Criteria Testing Laboratory 45901 Nokes Boulevard Sterling, VA 20166
Evaluation Team:	Abdul Qayyum (Lead Evaluator) Ken Dill Rick West Diann Carpenter
Validation Team:	Patrick Mallett Robin Medlock The MITRE Corporation 7515 Colshire Drive McLean, VA 22102-7508

4 SECURITY POLICY

The Security Policy of the TOE is enforced by the security functions of the TOE. These security functions are described below.

4.1 Audit

The TOE provides auditing record generation capabilities for digitally signing data and verifying the digital signature of data. The auditing record generation capabilities of the

TOE also report any integrity violations for verifications that are performed. It also identifies the specific data that has been modified.

Only signing and verification operations related to data stored in a database generate audit log records, however. No audit log records are generated for file or buffer signing and verification.

4.2 Digital Signature

The TOE provides the capability to perform digital signature operations which include digitally signing data and verifying digitally signed data. The TOE supports the defined digital signature operations on statically stored data within a database. The TOE additionally provides the capability to perform the defined digital signature operations against application-constructed data stored in memory buffers or files. The TOE utilizes the defined digital signature operations to integrate with third-party applications that require the use of the digital signature operations that the TOE provides.

The TOE provides non-repudiation of origin by providing the capability to verify the digitally signed data. Verification is possible because the TOE stores the signer's certificate with the data.

5 THREATS AND ASSUMPTIONS

5.1 Threats Addressed by the TOE

The Security Target identifies the following threats that the evaluated product addresses:

T.MODIFY	The integrity of data stored, processed, or transmitted may be compromised due to the unauthorized modification or destruction of the data or stored digital signatures by an attacker.
T.NO_LOG	A user may receive an integrity violation while verifying a digital signature and the integrity violation does not get recorded.
T.USER_DENY	A user denies having modified or inserted a database record that is digitally signed by that user.

5.2 Threats Addressed by the Environment

The Security Target identified the following threats that the environment addresses:

T.KEY_COMPROMISE	A user utilizes a non-FIPS 140-1 or non-FIPS 140-2 conformant cryptographic mechanism for generating a cryptographic key to be used with DBsign and the cryptographic key is compromised by an attacker.
T.NO_LOG	A user may receive an integrity violation while verifying a digital signature and the integrity violation does not get recorded.
T.AUDIT_SEQUENCE	An administrator is unable to distinguish the sequence of audit events and therefore cannot detect recent integrity violations.

5.3 Assumptions for the Environment

The Security Target identifies the following assumptions for the environment in which the TOE operates.

A.ADMIN	It is assumed that one or more authorized administrators are assigned who are competent to manage the TOE, the IT environment supporting the TOE, the security of the information the TOE contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security.
A.INSTALLER	It is assumed that the installer of the TOE is provided by Gradkell and has sufficient expertise and knowledge to properly install the TOE within its evaluated configuration.
A.LOCATE	The processing resources of the TOE are assumed to be located within controlled access facilities that will restrict unauthorized physical access.
A.USER_ID	It is assumed that the certificate user or certificate user's certificate authority has correctly associated the certificate user's user identity and certificate issuer with their certificate.

6 ARCHITECTURE INFORMATION

DBsign is a software TOE. At a minimum, DBsign consists of two physical computers. DBsign supports multiple clients to a server; however, at least one client is required to support the full functionality of DBsign. The first computer is the client, which includes an operating system, database application, DBsign, and its underlying hardware. The second computer is the server, which includes an operating system, an RDBMS, the DBsign Administration Tools, and its underlying hardware. The TOE also requires connectivity

between the client and server to support the digital signature operations performed by DBsign.

Figure 1 depicts the physical architecture of DBsign. The grayed rectangle labeled "DBsign", including the components DBsign API, DBsign Crypto Adaptor (DCA), and Query Module (QM), represents the TOE components and boundaries in relation to the non-TOE components. The non-TOE components of the client include the operating system, a database application, and its underlying hardware. The non-TOE components of the server include the operating system, RDBMS[1], DBsign Administration Tools, and the underlying hardware. In addition, the database protocol used to communicate between the client and server is also a non-TOE component

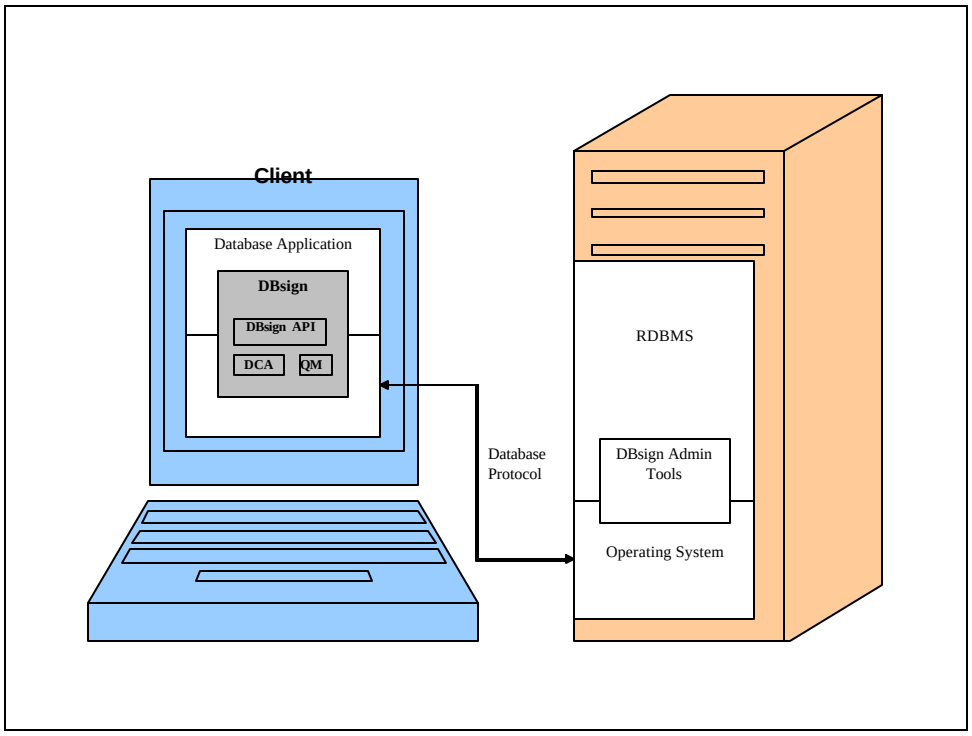

Figure 1 DBsign Client/Server Physical Architecture

7 DOCUMENTATION

During the course of the evaluation, the CCTL has access to an extensive amount of documentation and evidence.

[1] The audit data and DBS tables reside in the RDBMS, which is in the TOE environment,

7.1 Configuration Management Documentation

- Configuration Management for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0, and DBsign for OWF Applications Version 3.0, Version 1.3 Final, September 13, 2005.

7.2 Delivery and Operation Documentation

- Delivery Procedures for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0, and DBsign for OWF Applications Version 3.0, Version 0.3 Final, September 13, 2005.

7.3 Development Documentation

- Functional Specification and Correspondence for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0, and DBsign for Oracle Web Forms Applications Version 3.0, Version 0.41 Draft, revision 6,April 1, 2005.
- High-Level Design for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0, and DBsign for Oracle Web Forms Applications Version 3.0, Version 0.4 Draft, revision 4, November 24, 2004.
- DBsign Data Security Suite, Concepts Manual, Version 3.0, July 15, 2005.

7.4 Guidance Documentation

- DBsign for Client/Server Applications Installation Manual, Version 3.0, July 15, 2005
- DBsign for Client/Server Applications Integration Guide, Version 3.0, July 15, 2005
- DBsign Administration Tools Manual, Version 3.0, July 15, 2005.

7.5 Tests Documentation

- DBsign Automated Test Mappings.doc
- DBsign - CCTL functional testing results - Vendor Functional Test Results - HTML.zip, July 28th, 2005.
- DBsign 3.0 Test Plan, Procedures, and Correspondence Version 1.3 Draft, Revision 1050, May 12, 2005.

- DBsign for Client/Server Applications Version 3.0 Team Test Plan Version 5.0

7.6 Vulnerability Assessment Documentation

- Vulnerability Analysis for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0, and DBsign for OWF Applications Version 3.0, Version 0.3 Final, September 13, 2005.

7.7 Security Target

- DBsign for Client/Server Applications Version 3.0 Security Target, Version 1.0 Final, 13 September 2005.

8 EVALUATED TOE CONFIGURATION FOR CLIENT/SERVER APPLICATIONS

DBsign for Client/Server applications runs on the client system with the following operating systems and database clients:

- Microsoft Windows 98, Me, NT, 2000, XP, 2003
- Database client that supports DB2-CLI, JDBC, ODBC, OCI 7.0, OCI 8.0, or OCI 8i

DBsign for Client/Server Applications communicate with a database, running on the server, via a network protocol recognized by the database to retrieve data to be signed by the client. DBsign supports most Relational Database Management Systems (RDBMSs).

The test environment was configured to resemble a standard Government or Corporate environment where such a system would be used, although the TOE was not connected directly to the public Internet during testing. The test environment consisted of two Windows 2000 machines acting as host machines for "virtual machine software, which is discussed further below. One virtual machine encompassed the role of "Client" and the other encompassed the "Database Server". The test environment is described in Section 9.

9 IT PRODUCT TESTING

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

9.1 Developer Testing

The vendor test plan (DBsign 3.0 Test Plan, Procedures, and Correspondence 1.3) describes the functional testing required to verify the functional claims made in the ST. The Plan and Test Procedures do not address features or characteristics not covered in the ST, for example system performance and throughput. In addition, the Plan and Test Procedures represent full testing of the Security Functional Requirements and Security Functions.

Automated Testing

To expedite the testing process, the vendor developed software termed "DBsign Test Runner" software. The software aggregates test cases into a test suite, which automates execution of the vendor test procedures. The software is written in java and is executed on the "Client" The DBsign Test Runner software provides a GUI where the test suite can be executed and results viewed.

Virtual Machines

Virtual machines are computers that run on virtualized hardware. Software running within the VM, including the operating system, executes as if it is on real hardware. The vendor has incorporated virtual machines for the purpose of expediting the testing process. Two virtual machines representing a "Client" and "Server" were employed in the vendor test plan.

Pre-configured Test Environments

The vendor tests were executed against pre-configured test environments. Pre-configured test environments consist of various combinations of operating systems, applications, and databases that are pre-populated with test data and are implemented via virtual machines discussed above. The purpose is to reduce the time overhead required to setup "clean" environments for all iterations of the test procedures.

Test Execution and Java Code

Each test suite was executed referencing a configuration file. Parameters are defined in the configuration text file and can be changed manually to specify different data and to produce different results. In each line of the configuration file, the text string can be replaced as desired.

Once the parameters are defined, the series of tests run against them are specified in a master java code script. For each defined test in the java code, the environment is cleared, parameters are imported from the configuration file, whichever DBsign APIs are required to perform the test are called, the results of the test are checked, and results output directed to an HTML file.

There are six crypto functions checked by the tests: sign data defined by a template; verify signed data defined by a template; sign data in a buffer; sign a file; verify the signature applied to buffer data; and verify a signature applied to a file. Each DBsign operation also produces audit information, which can be manually checked to make sure auditing is functioning, or a java script test can be run to check auditing accuracy.

Some of the tests have dependencies. For example, when running a "verify signature" test, the corresponding "sign data" test must first be run. If checking auditing accuracy through the java code test, the other tests must have been run and must have produced the auditing activity.

The evaluation team used the vendor supplied testing environment as a basis for conducting its independent tests.

9.2 Evaluation Team Independent Testing

The evaluation team installed the TOE in the evaluated configuration using the CCTL's test lab. The evaluation team chose to run a subset all of the vendor tests. The subset was chosen to ensure adequate coverage for all security functional requirements. Some issues were noted during initial testing, and updates were provided by the vendor to correct the problems. The evaluation team then verified that the vendor test suite coverage was adequate, that the vendor test sets tested the security mechanisms and external interfaces of the TOE.

The evaluation team designed and ran a set of independent functional tests to augment the vendor testing. The team focused on the Digital Signature and Verification component, because it is the primary purpose for the product. The team tested digital signing claims as related to FCS_COP.1 using cryptographic key sizes not explicitly tested by the vendor. The team also tested non-repudiation claims as related to FCO_NRO.1.

9.3 Evaluation Team Penetration Testing

The evaluation team performed penetration testing by devising penetration tests, building on the developer vulnerability analysis. For some cases, the vendor had already provided the test as part of the vendor test suite. For other cases, the evaluation team produced its own tests. The Validation team agrees that this is an appropriate method given the nature of the TOE as a set of APIs.

10 RESULTS OF THE EVALUATION

The evaluation was conducted based on the Common Criteria (CC), Version 2.2, and the Common Evaluation Methodology (CEM), Version 2.2, and all applicable interpretations in effect on 7 June 2004. The evaluation confirmed that DBsign for Client/Server Applications Version 3.0 is compliant with the Common Criteria Version 2.2 functional requirements (Part 2) and assurance requirements (Part 3) for EAL2.

The details of the evaluation are recorded in the CCTL's evaluation technical reports, which consist of the following documents. A separate ASE (Security Target Evaluation) ETR was produced for the ST. Evaluation results for the remaining assurance families are presented in separate ETR documents for each family. The ETR for each family combines the evaluation results of three TOE evaluations: DBsign for Client Server Applications version 3.0, DBsign for HTML Applications version 3.0, and DBsign for Oracle Web Forms version 3.0.

- ASE Evaluation Technical Report for DBsign for Client/Server Applications Version 3.0, September 14, 2005.

- ACM_CAP.2 Evaluation Technical Report for DBsign for Client/Server Application Version 3.0, DBsign for HTML Application Version 3.0, and DBsign for OWF Application Version 3.0. September 14, 2005.
- ADO_DEL.1; ADO_IGS.1 Evaluation Technical Report for DBsign for Client/Server Application Version 3.0, DBsign for HTML Application Version 3.0, and DBsign for OWF Application Version 3.0. September 14, 2005.
- ADV_FSP.1; ADV_HLD.1; ADV_RCR.1 Evaluation Technical Report for DBsign for Client/Server Application Version 3.0, DBsign for HTML Application Version 3.0, and DBsign for OWF Application Version 3.0. September 14, 2005.
- AGD_ADM.1; AGD_USR.1 Evaluation Technical Report for DBsign for Client/Server Application Version 3.0, DBsign for HTML Application Version 3.0, and DBsign for OWF Application Version 3.0. September 14, 2005.
- ATE_COV.1; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for DBsign for Client/Server Application Version 3.0, DBsign for HTML Application Version 3.0, and DBsign for OWF Application Version 3.0. September 14, 2005.
- AVA_SOF.1; AVA_VLA.1 Evaluation Technical Report for DBsign for Client/Server Application Version 3.0, DBsign for HTML Application Version 3.0, and DBsign for OWF Application Version 3.0. September 14, 2005.

The validation team followed the procedures outlined in the CCEVS Scheme Publication #3, *Guidance to Validators of IT Security Evaluations*. The validation team observed that 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 team's results are correct and complete.

11 VALIDATOR COMMENTS AND RECOMMENDATIONS

The validator observations support the evaluation team's conclusion that the DBsign for Client/Server Applications, Version 3.0, meets the claims stated in the Security Target.

The audit logging feature may be enabled or disabled by the administrator. However, the evaluated configuration of the TOE requires, at a minimum, for the audit logging feature to be enabled to audit the successful and failed signature generation and signature verification processes. Also note that only signing and verification operations related to data stored in a database generate audit log records. No audit log records are generated for file or buffer signing and verification.

The consumer is reminded that the following features are not evaluated:

- User policy feature

The consumer is reminded that the IT environment must protect the following:

- User's private key
- DBsign system tables, which reside in the environment RDBMS

- DBsign audit tables, which reside in the environment RDBMS

12 SECURITY TARGET

The Security Target is identified here by reference.

· *DBsign for Client/Server Applications Version 3.0 Security Target, Version 1.0 Final, 13 September 2005.*

13 BIBLIOGRAPHY

The Validation Team used the following documents to produce this Validation Report:

[1] *Common Criteria for Information Technology Security Evaluation*, Parts 1-3, Version 2.2, January 2004.

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

[3] CCIMB Interpretations, as of June 7, 2004.

[4] Common Criteria Evaluation and Validation Scheme for IT Security, Scheme Publication #3, Version 1.0, January 2002.

[5] *DBsign for Client/Server Applications Version 3.0 Security Target*, Version 1.0 Final, 13 September 2005.

[6] *ASE Evaluation Technical Report for DBsign for Client/Server Applications Version 3.0*, September 14, 2005.

[7] *ACM_CAP 2,.Evaluation Technical Report for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0 and DBsign for OWF Applications Version 3.0*, September 14, 2005.

[8] *ADV_FSP.1; ADV_HLD.1; ADV_RCR.1, Evaluation Technical Report for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0 and DBsign for OWF Applications Version 3.0*, September 14, 2005.

[9] *ADO_DEL.1; ADO_IGS.1, Evaluation Technical Report for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0 and DBsign for OWF Applications Version 3.0*, September 14, 2005.

[10] *AGD_ADM.1; AGD_USR.1, Evaluation Technical Report for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0 and DBsign for OWF Applications Version 3.0*, September 14, 2005.

[11] *ATE_COV.1; ATE_FUN.1; ATE_IND.2 Evaluation Technical Report for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0 and DBsign for OWF Applications Version 3.0*, September 14, 2005.

[12] *AVA_SOF.1; AVA_VLA.1 Evaluation Technical Report for DBsign for Client/Server Applications Version 3.0, DBsign for HTML Applications Version 3.0 and DBsign for OWF Applications Version 3.0*, September 14, 2005.