National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Metastorm BPM v9.1.1.3

Report Number: CCEVS-VR-VID10370-2012
Dated: 10 January 2012
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jim Brosey, Lead Validator

Olin Sibert, Senior Validator

Jean Petty, Lead Validator

Bradford O'Neill, Senior Validator

Common Criteria Testing Laboratory

Quang Trinh, Lead Evaluator
Julie Cowan
Science Applications International Corporation (SAIC)
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Metastorm BPM v9.1.1.3, hereafter refer to as Metastorm BPM.

The Validation Report presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of Metastorm BPM was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory in the United States and was completed on December 2011.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by SAIC CCTL. The ETR and test report used in developing this validation report were written by SAIC. The evaluation team determined the product to be Part 2 conformant and Part 3 conformant, and meets the assurance requirements of EAL4 augmented with ALC_FLR.1. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE is Metastorm BPM v9.1.1.3 provided by Metastorm, Inc. The TOE provides the ability to view and manage information, activities, and instructions that can be used to automate a business process, for example a manager approving a staff member's form for a travel request. The TOE is an IT enabled Business Process Management software product supported on Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2. The TOE manages and tracks business processes flow and data in real time.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

During this validation, the Validators determined that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target (ST). Therefore, the Validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

2 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 EAL4 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;
- The Protection Profile to which the product is conformant; and
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Metastorm BPM v9.1.1.3
Protection Profile	None
ST	Metastorm BPM 9.1 Security Target, Version 0.13, 9 January 2012
Evaluation Technical Report	Evaluation Technical Report For Metastorm BPM 9.1 Part II (Proprietary). Version 1.1, 17 November 2011
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, September 2007
Conformance	CC Part 2 conformant and Part 3 conformant, EAL4 augmented with

Item	Identifier
Result	ALC_FLR.2
Sponsor	Metastorm, Inc.
Developer	Metastorm, Inc.
Common Criteria Testing Lab (CCTL)	Science Applications International Corporation 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Science Applications International Corporation: Quang Trinh, Julie Cowan
Validation Body	NIAP CCEVS: Jim Brosey, Lead Validator Olin Sibert, Senior Validator

3 Organizational Security Policy

This section summarizes the security functions provided by Metastorm BPM. It is based on information provided in the Security Target.

3.1 Security audit

The TOE generates audit events as each component of the TOE performs actions on deployed projects. The records of audited events are saved by the TOE in the database for later retrieval and reviewed by administrative users through an audit trail form. This audit trail form presents records in a manner determined by a project's designer and can be constructed to permit searching and/or sorting of audit records.

The TOE provides administrators with a way to view audit records created by the TOE.

3.2 User Data Protection

The TOE can control access to objects called forms and folders using ACLs specific to each form and folder. A business processes is comprised of folders that transition between stages through actions. A folder is a unique instance of a business process. A folder contains one or more forms. A form contains fields defining specific information that pertains to an instance of the business process.

When a business process is designed, the designer chooses the users or roles that are permitted to have access to a given folder, form or field. ACLs are used to define permissions on folders and forms. Fields on a form are either visible or not, depending upon the 'Visibility Depends On' property of the field. If the field is visible the user has the ability to modify or use the field. Visibility can be restricted based upon role.

3.3 Identification and authentication

The TOE defines users in terms of the security attributes user name, password, and role. The TOE provides its own username and password authentication mechanism that it uses to

authenticate users. While the product supports the use of additional authentication mechanisms (e.g., LDAP, RADIUS), only the local, TOE-defined username/password mechanism is supported in the evaluated configuration. In order to access the TOE, a user account including a user name and password must be created for the user. The TOE maintains both administrator and user roles.

3.4 Security management

The TOE provides applications and web-based administration forms that can be used to manage the TSF. The applications and forms include those that can perform the following management functions:

- Design and deploying of business process projects,
- Management of subjects and authentication data,
- Management of objects, and
- Management of session inactivity settings.

The TOE ensures that only an administrator can login and perform administrative management function. The TOE recognizes several roles: a process designer, an administrator, a user, and designer-specified user roles.

3.5 Protection of the TSF

The TOE restricts access to both its administrative and non-administrative interfaces. The TOE ensures that only an administrator can login and perform administrative management functions. The TOE also utilizes support in the environment (e.g., the database, the web server, and the operating system) to protect data stored in the database, to communicate with network entities, and to protect communications with users. This information is provided in support of the security assurance requirements, more specifically the architecture requirements for non-bypassability.

3.6 TOE Access

The TOE can terminate inactive interactive user sessions. The TOE relies on a timestamp provided by the operating system in the environment in order to determine if a session has become inactive.

4 Assumptions and Clarification of Scope

The statement of TOE security environment (now refer to as Security Definition Problem) describes the security aspects of the environment in which it is intended that the TOE will be used and the manner in which it is expected to be deployed. The statement of TOE security environment therefore identifies the assumptions made on the operational environment and the intended method for the product, organizational security policies which the product is designed to comply, and threats that the TOE is designed to counter.

Following are the assumptions identified in the Security Target:

- The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- The TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.
- The environment will provide protection of TSF data transmitted between the TOE and the database, as well as communication between the MBPM web application and the MBPM engine.
- The environment will provide a storage capability for audit records that protects audit records and makes them available for the TOE to retrieve.

Following are the organizational security policies levied against the TOE and its environment as identified in the Security Target.

- Access controls will ensure that only those users who have been authorized to access the protected information within the TOE will be able to do so.
- All users must be identified and authenticated prior to accessing any controlled resources.
- The TOE must limit the access to information in protected resources to those authorized users who have a need to know that information.
- The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

Following are the threats identified in the Security Target:

- An authorized administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
- An unauthorized user, process, or external IT entity may masquerade as an authorized entity to gain access to data or TOE resources.
- A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
- A user may gain unauthorized access (view, modify, delete) to user data.
- Persons may not be accountable for the actions that they conduct, thus allowing an attacker to escape detection.

5 Architectural Information[1]

A business process (project) is comprised of processes that define folders, stages and actions. A folder is a unique instance of a business process (project). A folder contains one or more forms. A form contains information relating to an instance of the business process (project). The TOE can control access to objects called forms and folders. The

[1] Extracted from SAIC Final ETR Part I Version 1.0, 28 January 2011

TOE provides users with interfaces that can view and manage business processes (projects).

The TOE has the ability to restrict user access to forms and folders. Users are assigned to a role. Forms and folders have associated with them Access Control Lists (ACLs). The ACL identifies a user and/or role and the actions that the user and/or role are permitted to perform. The ACL is used to make access control decisions for the associated object.

Users access the TOE using a web browser in the environment. The web browser utilizes the TOE's web interface. Users are required to provide a user name and password to the TOE before a session with the TOE can be established.

Administrative users access the TOE's Administration Tool using a web browser in the environment. Administrators using this application are required by the TOE to provide a user name and password to the TOE before a session with the TOE can be established.

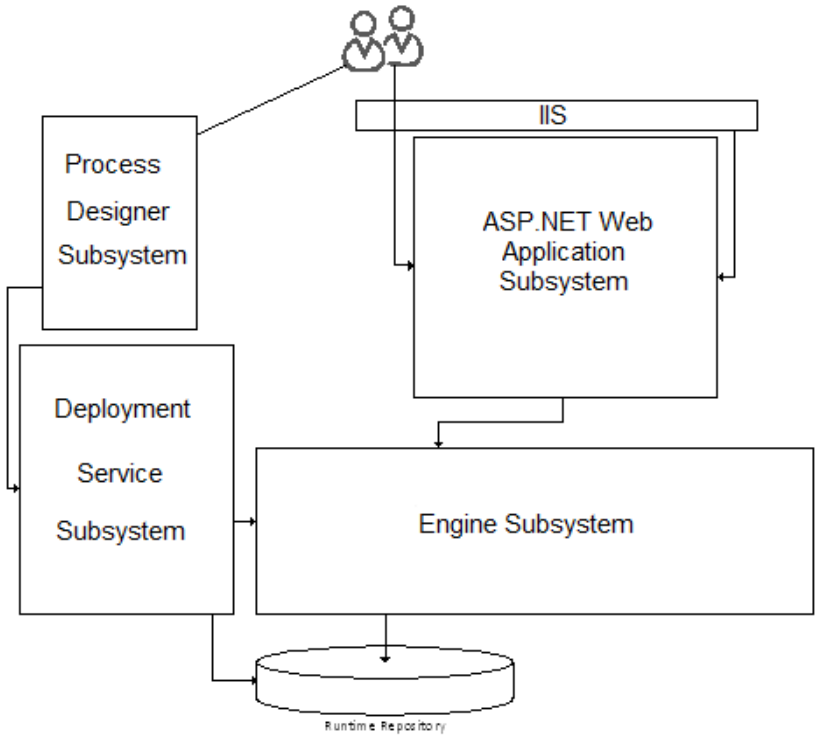


Figure 1: Metastorm BPM TOE Components

The TOE in its intended environment can be described in terms of the following subsystems:

- MBPM ASP.NET Web Application (web server plug-in) subsystem – This subsystem is an ASP.NET application for Microsoft Internet Information Services

(IIS) web server. This subsystem presents a web interface to users and administrators through IIS. User web page activity is translated into XML messages that are exchanged with the MBPM Engine subsystem. Administrators utilize MBPM Administrator Forms to manage the TOE.

  - MBPM Administrator Forms – The MBPM Admin Forms provide interfaces to perform security relevant administrative operations through the use of a Metastorm provided business process model. This model contains 11 Admin Forms designed specifically to support functionality described by this Security Target. The following is a list of these forms.
    - Assign Roles to User Form
    - Assign Users to Role Form
    - Audit Trail – Deployment
    - Audit Trail – Processes
    - Change Password Form
    - Edit Server Settings Form
    - Event Log – Metastorm Apps
    - Authentication Log Form
    - Process Log Form
    - Create, Delete and Update Users Form
    - Update Session Timeout Form

- MBPM Engine subsystem – This subsystem is a server application that evaluates and processes MBPM transaction requests from the end users. This subsystem processes Business Process Management logic that is defined by administrators and is operated upon by end users. The result is that this subsystem performs and controls work flow management functions.

- MBPM Deployment Service Subsystem – The Deployment Service subsystem is responsible for validating and then preparing process models for execution. The Deployment Service interprets the process models and writes the appropriate process metadata into the process repository, in a format that is by the Process Engine. By acting as an intermediary between the Designer and the runtime repository, it also allows users to deploy process models without needing direct access permissions to the DBMS. It also has the secondary ability of storing copies of the Designer libraries and projects that contain the process models, for later retrieval and loading back into the Designer

- MBPM Process Designer application – This application provides interfaces to create and modify procedures and their components (forms, folders). This application is accessed using the interfaces provided by the application.

The environment the TOE runs in is composed of the following.

- Operating system – Provides runtime environment for MBPM Engine subsystem and MBPM Engine administrator console subsystem (as well as database, web server, and web browser).
- Database – Stores MBPM Engine subsystem and MBPM Engine administrator console subsystem configuration data.
- Web server – Provides runtime environment for MBPM ASP.NET Web Application subsystem. The web server is also expected to be configured such that web pages served from the MBPM ASP.NET Web Application are provided only through the HTTPS protocol.
- Web browser – Provides a web-based client interface to access MBPM Engine subsystem services using the MBPM ASP.NET Web Application subsystem.

6 Documentation

Following is a list of the evaluation evidence, each of which was issued by the developer (and sponsor).

6.1 Design documentation

Document	Version	Date
Metastorm Enterprise 9.1 Security Architecture Document	Version 0.2	9/02/2011
Metastorm Enterprise 9.1 Functional Specification	Version 0.4	1/05/2012
Metastorm Enterprise 9.1 TOE Design Specification	Version 0.4	9/02/2011

6.2 Guidance documentation

Document	Version	Date
Metastorm BPM Version 9.1 Administration Guide		6/2011
Metastorm BPM Version 9.1 Designer User Guide		6/2011
Metastorm BPM Version 9.1 Installation Guide		6/2011
Metastorm BPM® Release 9.1 Installation Prerequisites		6/2011
Metastorm BPM Version 9.1 Release Notes		6/2011
Metastorm BPM® Release 9.1 Supported Environments		6/2011
Metastorm BPM Version 9.1 Using Metastorm BPM with Internet Explorer Guide		6/2011
Metastorm BPM Version 9.1 Web Client Configuration Guide		6/2011
Metastorm BPM Version 9.1.1.3 Release Notes	9.1 SR1	
Using Metastorm BPM in the Common Criteria Certification Configuration Documentation Addendum	Version 2.3	11/29/2009

6.3 Configuration Management and Lifecycle documentation

Document	Version	Date
Metastorm BPM Configuration Management	Version 1.0	1/27/2010
Metastorm BPM Delivery and Operating	Version 1.4	11/28/2011
Metastorm BPM Development Security	Version 1.0	1/27/2010
Metastorm BPM Flaw Remediation	Version 1.0	1/14/2010
Metastorm BPM Life-Cycle Definition	Version 1.1	1/14/2010
Actual logs, video evidence, CM records, CI lists	See ETR	

6.4 Test documentation

Document	Version	Date
Metastorm BPM 9.1 Tests	Version 0.4	10/03/2011
CCC Test Mappings	Version 0.3	
Metastorm BPM User Interfaces and Supporting Applications		
Metastorm BPM v91 ATE-COV-FUN v0.2 Test Record	Version 0.2	9/12/2011
Actual Test Scripts Actual Test Results + Screenshots	See ETR	

The actual test results have been submitted to the evaluation team, as log files.

6.5 Security Target

Document	Version	Date
Metastorm BPM 9.1 Security Target	Version 0.13	1/09/2012

7 IT Product Testing

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

7.1 Developer Testing

The developer tested the interfaces identified in the functional specification and mapped each test to the security function and security functional requirement. The scope of the developer tests included all the TSFI and consisted of manual and automated tests. The testing covered the security functional requirements in the ST including: Security Audit, User data protection, Identification and Authentication, Security Management, Protection of the TSF, and TOE Access. All security functions were tested and the TOE behaved 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 re-ran appropriately 40% of the developer's manual tests (testing the TSFIs) and automated test suite (testing the internal interfaces). The manual test cases focus mostly on verification of the external TSFIs while the automated test cases verify the security behaviors from the internal and programmatic interface. In addition to re-running the developer's tests, the evaluation team developed a set of independent team tests to address areas of the ST that did not seem completely addressed by the developer's test suite, or areas where the product was updated. All independent team tests were run as manual tests.

The vendor provided the TOE software and hardware for the test environment.

The following hardware and software necessary to create the test configuration:

TOE Software

- BPM 9.1 Web Extensions
- BPM 9.1 Process Engine
- BPM 9.1 Deployment Service
- BPM 9.1 Designer application

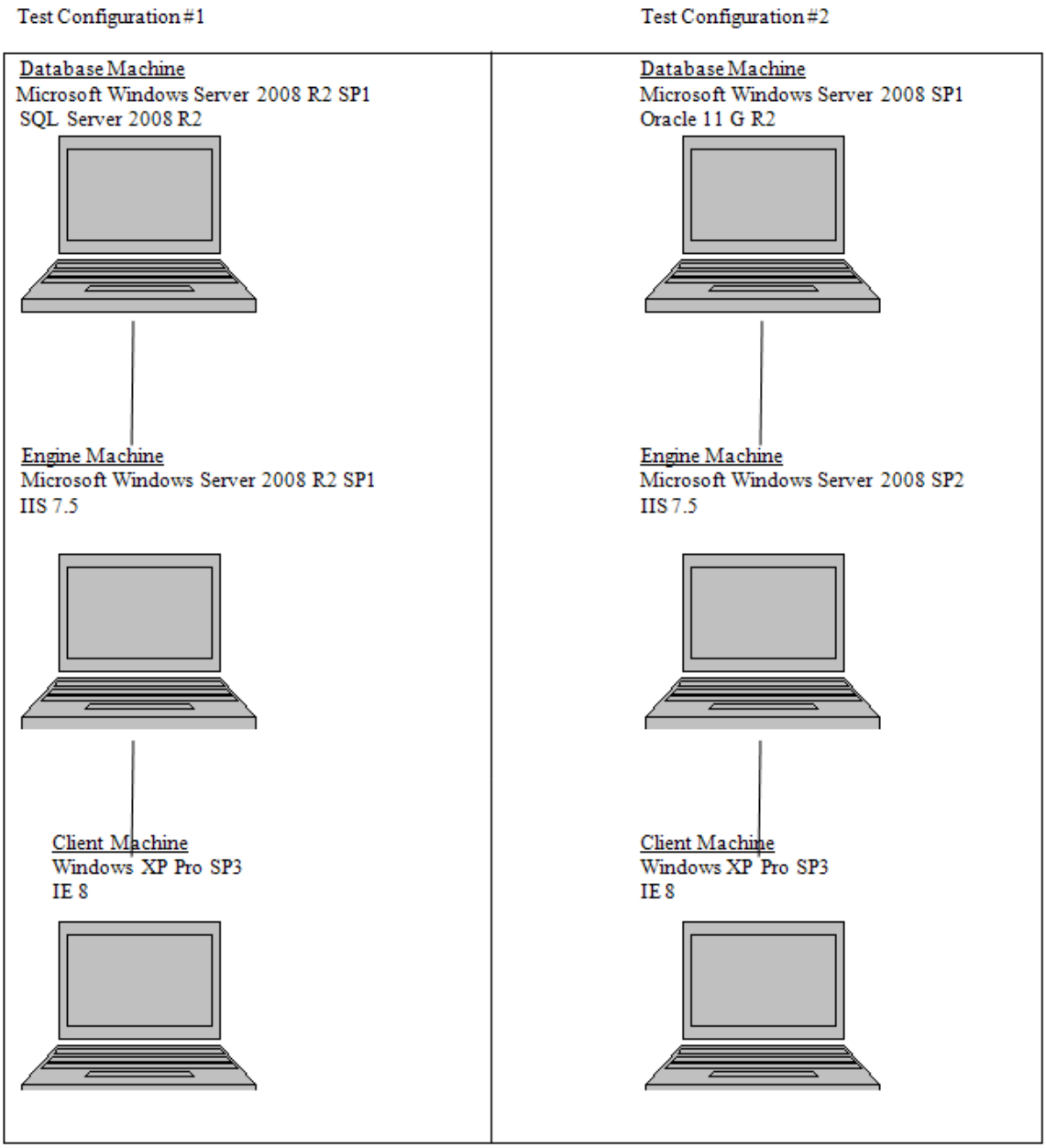
Test configuration #1:

- Microsoft Windows Server 2008 R2 SP1
- Microsoft IIS 7.5
- Microsoft SQL Server 2008 R2
- Microsoft IE 8

Test configuration #2:

- Microsoft Windows Server 2008 SP2
- Microsoft IIS 7.5
- Oracle 11 G R2 + ODAC 11.2.0.1.2
- Microsoft IE 8

During testing, the TOE or Metastorm BPM 9.1.1.3, was installed and configured on workstations with the operating system Windows Server 2008 SP2 and R2 SP1. The hot fix was applied to bring version to 9.1.1.3. Note that the TOE can run on any supported operating systems, irrespective of whether they are running in virtual machine environments or not. Metastorm, Inc. supports operating systems, not specific hardware configurations. The figure below shows the actual test environment configurations.



7.3 Penetration Testing

The evaluators developed penetration tests to address the User Input Validation, Network Sniffing, Web Vulnerability Scanning for OWASP Top Ten, Password Hashes Cracking, Session ID Manipulation, Predictable Session ID values, and Sensitive Data and Configuration Files Protection, as well as expanding upon the public search for vulnerabilities provided to the team by the sponsor. These tests identified no obvious vulnerabilities in the specific functions provided by the TOE.

The TOE performs good user input validation and the connections between the TOE and web client are protected by TLS. The CC evaluated configuration recommends configuring HTTPS instead of HTTP. In addition, the Session IDs are properly protected (encrypted) and the random number generator produces non-distinguishable random values for the Session ID. The *Using Metastorm BPM in the Common Criteria Certification Configuration Documentation Addendum* must be followed to put the TOE in the CC evaluated configuration and provide stricter file system permissions to protect sensitive data, files, and registry keys from unauthorized access.

8 Evaluated Configuration

The evaluated version of the TOE is identified as: Metastorm BPM v9.1.1.3.

The TOE comprised of the following four main software subsystems:

- MBPM ASP.NET Web Application subsystem
    - MBPM Administrator Forms
- MBPM Engine subsystem
- MBPM Deployment Service Subsystem
- MBPM Designer Application

These subsystems can be installed and configured on the same machine, or on separate machines with the exception of the Engine subsystem and Deployment Service Subsystem which must be on the same machine.

The TOE is a software product and when configured in Common Criteria mode, depends on the following:

- Operating system – Windows Server 2003 R2, Windows Server 2003 SP2, Windows Server 2008 SP2, Windows Server 2008 R2 SP1
- Database – Microsoft SQL Server 2005 SP4, Microsoft SQL Server 2008 SP1, Microsoft SQL Server 2008 R2, Oracle 10G R2, Oracle 11G R1, Oracle 11G R2
- Web server – Microsoft IIS 6 running on Windows Server 2003, Microsoft IIS 7, Microsoft IIS 7.5
- Web browser – IE 7, IE 8, Firefox

For greater security the later versions of these components are recommended.

When installed in a configuration that does not require the Common Criteria mode (Development/Test environments for example), any of the supported configurations identified in the *Metastorm BPM 9.1 Supported Environments* guide can be used.

The operating system in the operating environment provides an execution environment for components of the TOE, a reliable clock from which the TOE obtains time, network protocol support for communicating with web browsers as well as other resource

management traditional for operating systems (e.g., process isolation, timesharing of the CPU, and basic I/O).

The database provides a storage and retrieval mechanism utilized by components of the TOE.

The web server provides an execution environment for the MBPM ASP.NET Web Application component of the TOE. The web server also offers the HTTPS network protocol interface to a User's web browser. TOE guidance recommends the use of HTTPS.

The web browser acts as the user's GUI.

9 Results of the Evaluation

The evaluation was conducted based upon version 3.1 Revision 2 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each 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 validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL4 augmented with ALC_FLR.2" certificate rating be issued for Metastorm BPM.

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

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.4: Complete functional specification
	ADV_IMP.1: Implementation representation of the TSF
	ADV_TDS.3: Basic modular design
AGD: Guidance Documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-Cycle Support	ALC_CMC.4: Production support, acceptance procedures and automation
	ALC_CMS.4: Problem tracking CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_DVS.1: Identification of security measures

Requirement Class	Requirement Component
	ALC_LCD.1: Developer defined life-cycle model
	ALC_TAT.1: Well-defined development tools
	ALC_FLR.2: Flaw reporting procedures
ATE: Tests	ATE_COV.2: Analysis of coverage
	ATE_DPT.2: Testing: security enforcing modules
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.3: Focused vulnerability analysis
ASE: Security Target Evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

10 Validator Comments/Recommendations

The validation team observed that the evaluation was performed in accordance with the CC, the CEM, and CCEVS practices. The Validation team agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR. The validation team therefore recommends that the evaluation results be accepted.

11 Security Target

The Security Target is identified as Metastorm BPM 9.1 Security Target, Version 0.13, 9 January 2012. The document identifies the security functional requirements (SFRs) necessary to implement the TOE security policies. These include TOE security functional requirements. Additionally, the Security Target specifies the security assurance requirements necessary for EAL4 augmented with ALC_FLR.2.

12 List of Acronyms

ACL	Access Control List
ASP	Active Server Pages
BPM	Business Process Management
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HTTP	Hyper Text Transfer Protocol
LDAP	Lightweight Directory Access Protocol
RADIUS	Remote Authentication Dial in User Service
PP	Protection Profile
SAIC	Science Applications International Corporation
SSL	Secure Sockets Layer
SSO	Single Sign On
ST	Security Target
TLS	Transport Layer Security
TOE	Target Of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
VPL	Validated Products List

13 Glossary of Terms

Term	Definition
Actions	Metastorm BPM defines an *action* as the step or activity necessary to modify data and move a folder from one stage to the next. Actions may include activities such as: • Filling out a form • Logging a telephone call • Reviewing an attached file • Approving or denying a request. It is also possible to have actions that do not require human intervention, such as: • Determining the routing for a folder based on information available in a folder or in a database

Term	Definition
	• Raising or responding to a flag • Moving a folder after a timed event • Starting an external application Properties and formulas can be set in the MBPM Designer to accommodate a wide variety of possible actions.
Administration Forms	Administration forms can be used by the user to carry out administrative processes. Administration forms: • Do not start a process • Are not available for use in processes • Cannot access custom variables • Cannot access system folder variables • Are not associated with any folder • Cannot be renamed. Administration forms are automatically associated with a creation action that leads to an Archive stage.
Folder	A new folder, with a unique, system-generated ID, is created each time a new instance of the process is initiated. In this way, the database can track the information particular to each instance of a business process. A folder contains one or more pages (forms) of information relating to that instance of the process. This information may come from a variety of sources, such as: • Input by a user onto a form; • Data extracted from a database (internal or external); and • A file generated by another application.
Forms	Within Metastorm BPM, a user may create *forms*. These forms are used to gather and display information necessary to a business process.
Process	When a user designs a Metastorm project, it is represented through one or more *processes* (diagrams or process models), each illustrating the various steps required to complete a business process (the lifecycle of a folder). Each instance of the business process is called a *folder*, and the steps are called *actions*.
Project	Metastorm BPM views the information, activities, and instructions required to automate a business process as a *project*. In Metastorm BPM, the main component of a project is one or more processes. In addition to the processes, a project may contain forms, roles, flags, external tables, and actions. All of these components are stored in a single solution file.
Roles	Participants (users) in a process have roles assigned to them based on either their individual or group responsibilities. Assignments within a project are made based on these role designations.
Flags	Flags are used to start or continue parts of an automated business process. There are two important aspects to the concept of a flag in

Term	Definition
	Metastorm BPM: the Flag itself and the Flagged Action invoked by the flag.
External Tables	External tables can be used to store configuration data, reference table data, or any other data related to the project

14 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, Version 3.1, Revision 1, September 2006, CCIMB-2006-09-001.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, September 2007, CCIMB-2007-09-003.

[4] Common Methodology for Information Technology Security: Evaluation methodology, Version 3.1, Revision 2, September 2007, CCIMB-2007-09-004.

[5] Evaluation Technical Report for the Metastorm BPM 9.1 Part II (Proprietary), Version 1.2, 7 January 2012.

[6] Metastorm BPM 9.1 Security Target, Version 0.13, January 9, 2012.

[7] Common Criteria Evaluation and Validation Scheme, Publication #4, Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 September 2008.