National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Metastorm, Inc.
Baltimore, MD

Metastorm e-Work 6.6.1

Report Number:	**CCEVS-VR-06-0046**
Dated:	**2006-10-26**
Version:	**0.4**

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

Dr. Deborah Downs
The Aerospace Corporation
El Segundo, California

Common Criteria Testing Laboratory

Ms. Terrie Diaz, Lead Evaluator
Jasmine Maleki
Quang Trinh
Science Applications International Corporation
Columbia, Maryland

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the Metastorm e-Work 6.6.1 Security Target.

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Metastorm e-Work 6.6.1 from Metastorm, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in October 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2** and **Part 3 Conformant**, and meets the assurance requirements of Evaluation Assurance Level (EAL) 2.

The Metastorm e-Work 6.6.1 product is an IT enabled Business Process Management (BPM) software product that supports viewing and managing the information, activities, and instructions required to automate a business process that is called a procedure. The main component of a procedure is one or more maps. Maps are diagrams or process model logical constructs that depict business processes such as a manager approving a staff member's form for a travel request.

The Metastorm e-Work 6.6.1 TOE can control access to objects called forms and folders. Forms are used to define business process information in objects. Folders are collections of forms that represent logical constructs of business process model maps and diagrams. Combinations of forms and folders represent business processes (procedures) that the TOE can provide users interfaces with in order to view and manage.

The TOE users have to be assigned to a role, and Access Control Lists (ACLs) containing user and/or role identifiers are used to make access control decisions for a given object. Non-administrative users access the TOE using a web browser in the IT environment to access the TOE HTTP network protocol interface.

The Metastorm e-Work 6.6.1 product is composed of several components:

- e-Work Web Extensions.ISAPI (web server plug-in) subsystem – An Internet Server API (ISAPI) server library for Microsoft Internet Information Services web server that handles end user HTTP requests to the e-Work Engine component and supports processing of e-Work data using web browsers.
- e-Work Engine subsystem – A server application that evaluates and processes e-Work transaction requests from end users. Processes Business Process Management (BPM) logic is defined by administrators and used by end users to perform workflow management functions.
- e-Work Engine administrator console subsystem – Provides graphical user interface (GUI) Windows application interfaces to manage the e-Work Engine component. Includes the following subcomponents:

- System Administrator application – Provides interfaces to start/stop the e-Work Engine component and to configure authentication mechanisms. It is accessed using Windows Microsoft Management Console (MMC) interfaces.
- e-Work Designer application – Provides interfaces to create and modify existing procedures and their components (forms, folders). It is accessed using Windows application interfaces.
- Services Manager application – Provides interfaces to manage existing procedures (e.g. making a procedure available to users) and their components (forms, folders). It is accessed using Windows Microsoft Management Console (MMC) interfaces.
- Users and Roles application – Provides interfaces to manage users and user attributes. It is accessed using Windows application interfaces.
- Administrator Forms application – Provides interfaces to manage user session timeout.

This validation assumes the TOE has been configured as described in Section 1.1 of the ST. The supporting hardware, OSs, DBMSs, web servers and web browsers were not included in the scope of the evaluation.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Criteria for IT Security Evaluation (Version 2.2) [12][13][14]. 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 [16] and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, 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 SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level 2 have been met.

The technical information included in this report was obtained from the Evaluation Technical Report (ETR) Part 1 (non-proprietary) produced by SAIC [18], the Metastorm e-Work 6.6.1 Security Target [17], and research and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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.
- The organizations and individuals participating in the evaluation.

Table 2-1. Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Metastorm e-Work 6.6.1 comprised of the following components: • e-Work Web Extensions.ISAPI subsystem • e-Work Engine subsystem • e-Work Engine administrator console subsystem including the following subcomponents o System Administrator application o e-Work Designer application o Services Manager application o Users and Roles application o Administrator Forms application The Metastorm e-Work 6.6.1 TOE must be configured in accordance with the

Item	Identifier
	following Guidance Documents: • Metastorm e-Work 6.6.1, Designer User Manual, April, 2005 [2] • Metastorm e-Work 6.6.1, e-Work Concepts, April, 2005 [3] • Metastorm e-Work 6.6.1, Administration Guide, April 2005 [4] • Using Metastorm e-Work 6.6.1 in the Common Criteria Certification Configuration Documentation Addendum , Issue 1.1, September 28, 2006 [5] • Metastorm e-Work 6.6.1 Supported Environments, April 2005 [6] • Metastorm e-Work 6.6.1 Installation Prerequisites, April 2005 [10] • Metastorm e-Work 6.6.1 Release Notes, April 2005 [11]
ST:	*Metastorm e-Work 6.6.1 Security Target*, Version 1.0, 3 October, 2006 [17]
Evaluation Technical Report	• *Evaluation Technical Report for Metastorm e-Work 6.6.1, Part I (Non-Proprietary)*, Version 2.0, October 3, 2006 [18] • *Evaluation Technical Report Metastorm e-Work 6.6.1, Part II (Proprietary)*, Version 2.5, October 11, 2006 [19]
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.2 [12][13][14]
Conformance Result	CC Part 2 and CC Part 3 conformant
Sponsor	Metastorm, Inc., Baltimore, MD, USA
Developer	Metastorm, Inc., Baltimore, MD, USA
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD, USA
CCEVS Validator	Deborah D. Downs, The Aerospace Corporation, El Segundo, CA

2.1 Applicable Interpretations

No international or NIAP interpretations were applied to this evaluation.

3 Security Policy

The Security Functional Policies (SFPs) implemented by Metastorm e-Work 6.6.1 provide for authenticated administrative user access to specify the contents of and security policies on forms and folders and authenticated user access to the interfaces to the procedures represented in those forms and folders. Users who are owners of forms and folders may also specify their contents and the other users who can access them.

Note: Much of the description of the Metastorm e-Work 6.6.1 security policy has been extracted and reworked from the Metastorm e-Work 6.6.1 security Target [17].

3.1 User Data Protection

The TOE implements a Work Flow Access Control Policy for object access based on:

- user identities,

- object ownership,
- assigned roles, and
- Access Control Lists (ACLs).

The TOE objects subject to this policy are forms and folders. Forms are used to define business process information in objects. Folders are collections of forms that represent logical constructs of business process model maps and diagrams. Combinations of forms and folders represent business processes (procedures) that the TOE can provide users interfaces in order to view and manage. For example, an airline could model a ticket sales process that provides employee interfaces to justify, cancel or withdraw their travel requests.

The TOE has the ability to restrict update access to the design of forms and folders to their owners and to administrators. Users may be assigned to an ACL; ACLs containing user identifiers are used to make access control decisions for a given object. Similarly, users may be assigned to a role, and ACLs containing user and/or role identifiers are used to make access control decisions for a given object.

Roles are a way of grouping users in an organization. A user can have any number of roles, and a role can be assigned to one or many users. Roles are created during the procedure design process and added to the e-Work database when a procedure is published. The procedure design process consists of creating maps (folders) and forms in order to build business rules that are used to automate business processes.

3.2 Identification and Authentication

The Metastorm e-Work 6.6.1 TOE defines users in terms of:

- user identity,
- authentication data, and
- roles.

The TOE provides its own login process where the user provides identity and password. While the product supports additional authentication mechanisms, only username/password in general is supported in the evaluated configuration. In order to access the TOE, an administrator must create a user account including a user name and password for the user.

Non-administrative users access the TOE using a web browser in the IT environment to access the TOE HTTP network protocol interface. The TOE authenticates the user using the supplied user name and password.

Administrative users access the TOE using e-Work Engine administrator console component Windows application graphical user interface (GUI) interfaces. As with all users, administrators are required to provide a user name and password before a session with the TOE can be established. But the administrator user name and password are forwarded to the database that verifies the password and thus authenticates the administrative user.

Note that the TOE does not implement any password composition rules or minimum password lengths. Administrative guidance is relied on to only ensure that when user accounts are created a minimum password length of eight printable characters is used.

3.3 Security Management

The Metastorm e-Work 6.6.1 TOE provides administrators with Windows application graphical user interface (GUI) interfaces to create and manage process flows, and to manage the security functions of the TOE. An administrator console can be logically described as the e-Work Engine administrator console component.

The e-Work Engine administrator console component interfaces include those that can perform the following management functions:

- management of subjects and authentication data
- management of objects
- management of session inactivity settings

Administrator console interfaces can only be called by administrators, with the exception of interfaces to manage objects, which can be called by object owners to modify owned object ACLs. Users that have been assigned the administrator role are considered authorized administrators, all others are simply users.

3.4 Protection of the TSF

The Metastorm e-Work 6.6.1 TOE enforces that a user without the necessary role is denied communication with the TOE. Users cannot proceed to use their TOE role until they have supplied a user name and password that corresponds to the TOE access list.

4 Assumptions

The following assumptions underlie the evaluation and use of Metastorm e-Work 6.6.1.

4.1 Usage Assumptions

It is assumed that the TOE will be installed, configured, managed and maintained in accordance with its guidance documentation.

4.2 Environmental Assumptions

A key environmental assumption is physical security, for it is assumed that the Metastorm e-Work 6.6.1 TOE will be located within controlled access facilities, which will prevent unauthorized physical access

Although not stated as an environmental assumption, it is required that the operating environment will provide a reliable time source to enable the TOE to enforce interactive timeout values. Also the environment will maintain the administrative user's identity and authentication data and will successfully authenticate the user before allowing any other TSF-mediated actions on behalf of that user.

4.3 Clarification of Scope

4.3.1 Overarching Policies

The security requirements enforced by the Metastorm e-Work 6.6.1 TOE were designed based on the following overarching security policies:

1. 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.
2. All users must be identified and authenticated prior to accessing any controlled resources.
3. The TOE must limit the access to information in protected resources to those authorized users who have a need to know that information.
4. 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.

4.3.2 Threats Countered and Not Countered

The TOE is designed to fully or partially counter the following threats:

- 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.

However, users of the TOE should be cautioned that:

- There is no explicit assumption about the security of the connections between the components of the TOE. Although the guidance documents recommend protection of those connections, without strong encryption or the equivalent they are at risk for sniffing and alteration of TOE data being conveyed on the connection.

4.3.3 Components that are not part of the TOE

It is important to note that the following components are not part of the TOE:

- Operating system – Provides a runtime environment for e-Work Engine component and e-Work Engine administrator console component (as well as the database, web server, and web browser components).

- Database – Stores the e-Work Engine component and the e-Work Engine administrator console component configuration data.
- Web server – Provides a runtime environment for e-Work Web Extensions.ISAPI component.
- Web browser – Provides a web-based client interface to access e-Work Engine component services using the e-Work Web Extensions.ISAPI component.

5 Architectural Information

Note: The following architectural description is based on the description presented in Evaluation Technical Report for the Metastorm e-Work, Part I and in the Metastorm e-Work 6.6.1 Security Target.

5.1 TOE Components

As noted before, the Metastorm e-Work 6.6.1 product is an IT enabled Business Process Management (BPM) software product that supports viewing and managing the information, activities, and instructions required to automate a business process that is called a procedure. The main component of a procedure is one or more maps. Maps are diagrams or process model logical constructs that depict business processes such as a manager approving a staff member's form for a travel request.

Note that Metastorm e-Work 6.6.1 is an application, layered on top of an unevaluated operating environment that includes an operating system, a database management system and hardware components.

The Metastorm e-Work 6.6.1 TOE consists of the following components:

- **e-Work Web Extensions.ISAPI (web server plug-in) subsystem** – An Internet Server API (ISAPI) server library for Microsoft Internet Information Services web server that handles end user HTTP requests to the e-Work Engine component and supports processing of e-Work data using web browsers.

  The Metastorm e-Work 6.6.1 web server plug-in requires the underlying operating system, web server and web browser to provide protection to the TOE. The underlying operating system is considered part of the environment.

- **e-Work Engine subsystem** – A server application that evaluates and processes e-Work transaction requests from end users. Processes Business Process Management (BPM) logic defined by administrators and used by end users to perform workflow management functions.

  The Metastorm e-Work 6.6.1 Engine requires the underlying operating system, web server, web browser, and database management system (DBMS) to provide protection to the TOE. The underlying operating system and DBMS is considered part of the environment.

- **e-Work Engine administrator console subsystem** – Provides graphical user interface (GUI) Windows application interfaces to manage the e-Work Engine component.

  The Metastorm e-Work 6.6.1 Engine requires the underlying operating system, web server, web browser, and database management system (DBMS) to provide protection to the TOE. The underlying operating system, DBMS and web server are considered part of the environment.

- The e-Work Engine includes the following subcomponents:
  - System Administrator application – Provides interfaces to start/stop the e-Work Engine component and to configure authentication mechanisms. It is accessed using Windows Microsoft Management Console (MMC) interfaces.
  - e-Work Designer application – Provides interfaces to create and modify existing procedures and their components (forms, folders). It is accessed using Windows application interfaces.
  - Services Manager application – Provides interfaces to manage existing procedures (e.g. making a procedure available to users) and their components (forms, folders). It is accessed using Windows Microsoft Management Console (MMC) interfaces.
  - Users and Roles application – Provides interfaces to manage users and user attributes. It is accessed using Windows application interfaces.
  - Administrator Forms application – Provides interfaces to manage user session timeout.

The Metastorm e-Work 6.6.1 Web Server Plug-in, Engine, and Administrator's Console run as applications on top of an operating system and depend on the services exported by the operating system to function. Metastorm e-Work 6.6.1 uses operating system services for process creation and manipulation; device and file processing; shared memory creation and manipulation; provision of the network stack up through the TCP layer; and security requests such as inter-process communication.

Metastorm e-Work 6.6.1 uses the DBMS to store procedure information, user identity and roles, and administrator identity and authentication data. Otherwise the DBMS is completely transparent to Metastorm e-Work 6.6.1 and it sees only the DBMS's user interfaces.

The web browser provides a web-based client interface to access the e-Work Engine component services using the e-Work Web Extensions.ISAPI component. The web server is used by Metastorm e-Work 6.6.1 to provide a runtime environment for the e-Work Web Extensions.ISAPI component. Otherwise the browser and server are completely transparent to Metastorm e-Work 6.6.1 and it sees only the user interfaces.

The hardware upon which the operating system runs is completely transparent to Metastorm e-Work 6.6.1; Metastorm e-Work 6.6.1 sees only the operating system's user interfaces.

The following table outlines the system requirements for Metastorm e-Work 6.6.1.

Metastorm e-Work 6.6.1		
Platform	**Support Enviroment**	**System Requirements**
Windows	2000 Professional SP4 2000 Server/Advanced Server SP4 SP Professional SP1a/SP2 Server 2003 Standard Server 2003 SP1	Specified in the installation and administration guidance.

5.2 TOE Boundaries

Figure 5-1 illustrates the Metastorm e-Work 6.6.1 TOE and its boundaries. This figure attempts to show that the underlying operating system, database management system, web server and web browsers (illustrated by their light brown color) which are all supported by the hardware are not part of the TOE for any of the three major TOE components and 5 sub-components (illustrated by their off-white color).

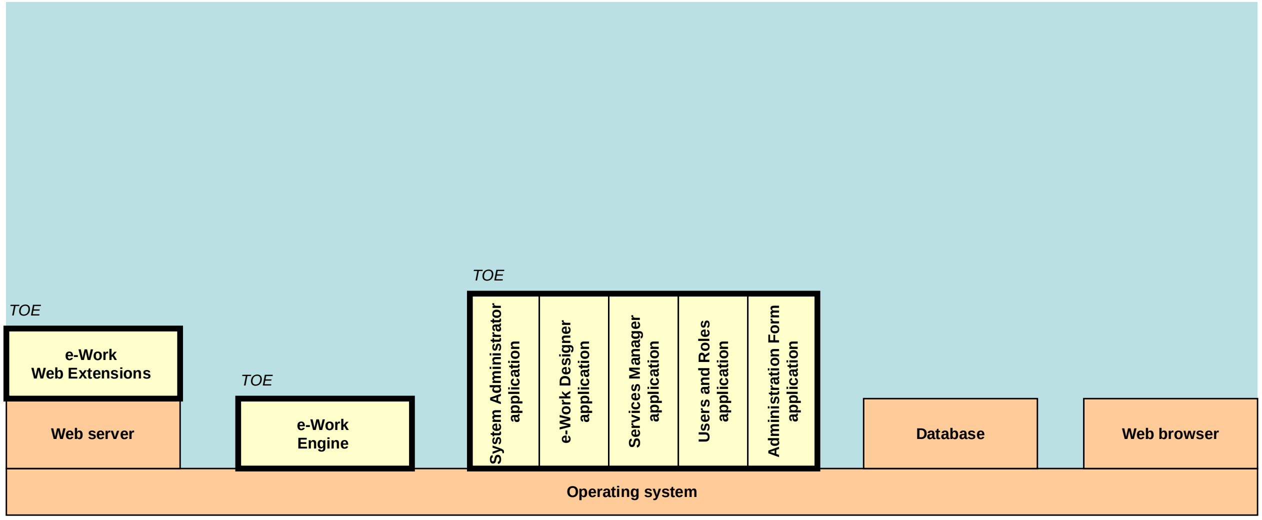
TOE
e-Work Web Extensions
Web server
TOE
e-Work Engine
TOE
System Administrator application
e-Work Designer application
Services Manager application
Users and Roles application
Administration Form application
Database
Web browser
Operating system

Figure 5-1. Boundaries of the Metastorm e-Work 6.6.1 TOE

In terms of logical boundaries, the following table enumerates the division between services provided *by* the TOE and services provided *to* the TOE from the Operating Environment:

Functional Area	Services Provided *By* The TOE	Services Provided *To* The TOE By The Operating Environment
User Data Protection	The TOE implements a Work Flow Access Control Policy for object access based on: • user identities, • object ownership, • assigned roles, and Access Control Lists (ACLs).	Underlying database used to store user identity, role, and object ownership, administrator identity and authentication data.
Identification and Authentication	Identification and authentication provided by Metastorm e-Work 6.6.1	TOE requests identification and passwords for all users. TOE authenticates non-administrative users. Administrators are authenticated by the database in the IT environment.
Security Management	Graphical user interfaces that create and manage process flows, and to manage the security functions of the TOE. The e-Work Engine administrator console component interfaces include those that can perform the following management functions: • management of subjects and authentication data • management of objects • management of session inactivity settings.	Underlying database used to store configuration information, and protection thereof. Environment provides accurate clock to time session inactivity.
Protection of the TOE	The Metastorm e-Work 6.6.1 TOE enforces that a user without the necessary role is denied communication with the TOE. Users cannot proceed to use their TOE role until they have supplied a user name and password that corresponds to the TOE access list.	Protection of the TOE executable and process data spaces.

5.3 IT Security Environment

Metastorm e-Work 6.6.1 requires an IT environment that protects the TOE (and its resources) with at least the same degree of assurance as that claimed by the TOE. The IT environment provides an accurate clock to time session inactivity. It also requires the environment to provide a database management system, web server and web browser.

6 Documentation

The following documentation was used as evidence for the evaluation of Metastorm e-Work 6.6.1. Documentation that is delivered in hardcopy to the customer with the product is indicated with an "X" in the "Dlvrd" column. Those documents with nothing in the "Dlvrd" column are not available to the customer.

6.1 Design documentation

Document	Dlvrd	Revision	Date
Metastorm e-Work 6.6 Design		0.3	2006-05-08

6.2 Guidance documentation

Document	Dlvrd	Revision	Date
Metastorm e-Work 6.6, Designer User Manual	X		2005-07
Metastorm e-Work 6.6, e-Work Concepts	X		2005-07
Metastorm e-Work 6.6, Administration Guide	X		2005-07
Metastorm e-Work 6.6, Using e-Work with Internet Explorer	X		
Using Metastorm e-Work 6.6 in the Common Criteria Certification Configuration, Documentation Addendum	X	1.1	2006-09-28
Metastorm e-Work 6.6 Supported Environments	X	(none)	2005-04

6.3 Configuration Management and Lifecycle documentation

Document	Dlvrd	Revision	Date
Metastorm e-Work Source Control Procedures		1.1	2005-09-25
Metastorm e-Work Product Lifecycle		1	

6.4 Delivery and Operation documentation

Document	Dlvrd	Revision	Date
Metastorm e-Work, Delivery and Operating Documentation	X	0.3	2006-09-01
Metastorm e-Work 6.6 Installation Perquisites	X		2005-07
Metastorm e-Work 6.6 Release Notes	X		2005-07
Metastorm e-Work 6.6 Installation Guide	X		2005-07

6.5 Test documentation

Document	Dlvrd	Revision	Date
Metastorm e-Work 6.6 Tests		0.13	2006-08-21
Metastorm e-Work 6.6 Test Record 20060817 (an Excel Spreadsheet)			2006-08-17

6.6 Vulnerability Assessment documentation

Document	Dlvrd	Revision	Date
Metastorm e-Work 6.6 Vulnerability Analysis		0.2	2006-10-02

6.7 Security Target

Document	Dlvrd	Revision	Date
Metastorm e-Work 6.6.1 Security Target		1.0	2006-10-03

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Plan, contained in Part II of the ETR, and has been reviewed to ensure it does not contain vendor proprietary information.

7.1 Developer Testing

Evaluator analysis of the developer’s test plans, test scripts, and test results indicated that the developer’s testing is adequate to satisfy the requirements of EAL2.

The developer’s tests of TOE security functions were provided by a series of manual tests. The actual results include screenshots used in exercising the test and a test record (Excel spreadsheet) that identifies each test case reference number with a pass/fail result. In addition each test procedure document included instructions for the repeatable execution of the tests, including a description of any requirements for establishing the test environment for each test as well as a description of how to actually execute each test and verify its results against the expected results.

The evaluation team verified that the test coverage was suitable through analysis of the developer-provided test documentation. Metastorm’s approach to security testing is requirement based. Each test case is subdivided into security functions and each test procedure targets the specific behavior associated with that security function.

Analyzing the functionalities addressed in the high-level design and associating test cases that cover the addressed functionalities address test depth. Each function maps the appropriate test cases and the rationale demonstrates why the test cases cover that particular function.

The developer provided the evaluation team with actual results for their testing of the product. The evaluation team analyzed the provided actual results against the results obtained by the evaluation team by running the entire set of the test cases. The results obtained were consistent with identified expected results.

7.2 Evaluation Team Independent Testing

In addition to developer testing, the CCTL conducted its own suite of tests. The evaluation team tested the product on the following platforms and confirmed that minimum configuration specified by the installation/administration guidance was used:

- Test Configuration #1:
  - Microsoft Windows 2003 SP1
  - Microsoft IIS 6
  - Microsoft SQL Server 2000 SPE (same machine)
  - Microsoft IE 6 SP2
- Test Configuration #2:
  - Microsoft Windows 2003 SP1
  - Microsoft IIS 6
  - Oracle 9R2 (same machine)
  - Microsoft IE 6 SP2

The CCTL verified that each of these platforms was running the TOE version of the firmware and the software. The CCTL installed the TOE and configured it in accordance with the provided guidance.

The evaluation team developed independent tests based on perceived gaps or areas of weakness in the developer's test suite, based on the preceding coverage and depth analyses. The focus was placed upon areas where the developer test documentation did not cover completely. The validator reviewed these independent tests and felt that they provided sufficient supplemental coverage to the vendor tests. The evaluation team used the exact configuration documented in the vendor test documentation, and uses the vendor test subset was to perform the team test. The evaluation team also used the same test tools documented in the vendor test documentation to perform the team test subset.

These tests identified some discrepancies between the actual implementation and the implementation documented. The vendor has updated the documentation.

7.3 Evaluation Team Penetration Testing

The CCTL also conducted penetration testing, using the same setup used for the independent team tests.

Prior to developing its tests, the CCTL followed well-established penetration test development procedures. This effort considered design documentation evaluation, guidance documentation evaluation, test documentation evaluation, code review, vulnerability analysis evaluation. It was revisited subsequent to the running of a portion of the vendor test subset. Therefore, it took advantage of TOE knowledge gained from each of these activities.

This resulted in small number of penetration tests. The validator reviewed these tests, and felt that they adequately explored areas of potential vulnerability. Execution of these tests resulted in some documentation clarifications, but identified no security vulnerabilities.

8 Evaluated Configuration

The evaluated configuration of Metastorm e-Work 6.6.1, as defined in the Security Target, consists of the following components:

1) e-Work Web Extensions.ISAPI (web server plug-in) subsystem
2) e-Work Engine subsystem
3) e-Work Engine administrator console subsystem

   The e-Work Engine includes the following subcomponents:

   - System Administrator application
   - e-Work Designer application
   - Services Manager
   - Users and Roles Administrator Forms

The Metastorm e-Work 6.6.1 TOE must be configured in accordance with the following Guidance Documents:

- Metastorm e-Work 6.6.1, Designer User Manual, April, 2005 [2]
- Metastorm e-Work 6.6.1, e-Work Concepts, April, 2005 [3]
- Metastorm e-Work 6.6.1, Administration Guide, April 2005 [4]
- Using Metastorm e-Work 6.6.1 in the Common Criteria Certification Configuration Documentation Addendum , Issue 1.1, September 28, 2006 [5]
- Metastorm e-Work 6.6.1 Supported Environments, April 2005 [6]
- Metastorm e-Work 6.6.1 Installation Prerequisites, April 2005 [10]
- Metastorm e-Work 6.6.1 Release Notes, April 2005 [11]

9 Results of the Evaluation

The evaluation was conducted based upon the Common Criteria (CC), Version 2.2, dated January 2004 [12][13][14]; the Common Evaluation Methodology (CEM), Version 2.2, dated January 2004; and all applicable International Interpretations in effect on April 1, 2004. The evaluation confirmed that the Metastorm e-Work 6.6.1 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 report, *Evaluation Technical Report for Metastorm e-Work 6.6.1*, Part 1 (Non-Proprietary) [18] and Part 2 (Proprietary) [19]. The product was evaluated and tested against the claims presented in the Metastorm e-Work 6.6.1 Security Target v1.0, 8 September 2006 [17].

The validator followed the procedures outlined in the Common Criteria Evaluation Scheme publication number 3 for Technical Oversight and Validation Procedures [16]. The validator has observed that the evaluation and all of its activities were in accordance with the Common Criteria, the Common Evaluation Methodology, and the CCEVS. The validator therefore concludes that the evaluation team's results are correct and complete.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the ASE product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified provided justification.

9.2 Evaluation of the Configuration Management Capabilities (ACM)

The evaluation team applied each EAL 2 ACM CEM work unit. The ACM evaluation ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation. To support the ACM evaluation, the evaluation team received Configuration Management (CM) records from Metastorm.

The validator reviewed the work of the evaluation team, and found that sufficient evidence that the evaluation was conducted in accordance with the requirements of the CEM and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Delivery and Operation Documents (ADO)

The evaluation team applied each EAL 2 ADO CEM work unit. The ADO evaluation ensured the adequacy of the procedures to deliver, install, and configure the TOE securely. The evaluation team ensured the procedures addressed the detection of modification while in transit. The evaluation team followed the Configuration Guide to test the installation procedures to ensure the procedures result in the evaluated configuration.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified provided justification.

9.4 Evaluation of the Development (ADV)

The evaluation team applied each EAL 2 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a high-level design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified provided justification.

9.5 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 2 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified provided justification.

9.6 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each EAL 2 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. To support the ALC evaluation, the evaluation team verified that the claimed procedures were followed during a site visit.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified provided justification.

9.7 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each EAL 2 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements.

Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification and high level design specification. The evaluation team performed all of the vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.8 Vulnerability Assessment Activity (AVA)

The evaluation team applied each EAL 2 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the developer misuse analysis, and the evaluation team's misuse analysis and vulnerability analysis, and the evaluation team's performance of penetration tests.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.9 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of a subset of the vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The evidence submitted for evaluation, as reported by the CCTL, did not consistently present good unique references (i.e., dates and version numbers). Although the CCTL did verify that this information was indeed under configuration control, the CM approach of the vendor could be strengthened if all evidence and items issued to customers had unique version numbers and dates.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as the *Metastorm e-Work 6.6.1 Security Target*, Version 1.0, 3 October 2006.

13 Bibliography

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

[1] Metastorm e-Work 6.6 *Design*, Version 0.3, May 8, 2006.

[2] Metastorm e-Work 6.6, *Designer User Manual*, April, 2005.

[3] Metastorm e-Work 6.6, *e-Work Concepts*, April, 2005.

[4] Metastorm e-Work 6.6, *Administration Guide*, April 2005.

[5] *Using Metastorm e-Work 6.6 in the Common Criteria Certification Configuration Documentation Addendum*, Issue 1.1, September 28, 2006.

[6] Metastorm e-Work 6.6 *Supported Environments*, April 2005.

[7] Metastorm e-Work *Source Control Procedures*, Issue 1.1, September 25, 2005.

[8] Metastorm e-Work *Product Lifecycle*, Version 2.

[9] Metastorm e-Work, *Delivery and Operating documentation*, Issue 0.3, September 1, 2006.

[10] Metastorm e-Work 6.6 *Installation Prerequisites*, April 2005.

[11] Metastorm e-Work 6.6 *Release Notes*, April 2005.

[12] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model*, Version 2.2, Revision 256, January 2004.

[13] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements*, Version 2.2, Revision 256, January 2004.

[14] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements*, Version 2.2, Revision 256, January 2004.

[15] Common Criteria Project Sponsoring Organisations. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, Version 2.2, Revision 256, January 2004.

[16] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[17] Science Applications International Corporation, *Metastorm e-Work 6.6.1 Security Target,* Version 1.0, 3 October, 2006

[18] Science Applications International Corporation, *Evaluation Technical Report for the Metastorm e-Work, Part I (Non-Proprietary)*, Version 2.0, 3 October 2006

[19] Science Applications International Corporation, *Evaluation Technical Report for the Metastorm e-Work, Part II (Proprietary)*, Version 2.5, 11 October 2006

Note: This document was used only to obtain the description of the test effort.