National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Microsoft Windows
Rights Management Services (RMS) 1.0 SP2

Report Number:	**CCEVS-VR-07-0057**
Dated:	**8 August 2007**
Version:	**1.2**

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

Rick Murphy
Noblis
Jerry Myers
Aerospace

Common Criteria Testing Laboratory

Tony Apted
Mark Braga
Rachel Lisi
Jean Petty
Quang Trinh
Roland Zeender
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Microsoft Windows Rights Management Services (RMS) 1.0 SP2 (the Target of Evaluation, or TOE). 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 May 2007. 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 **Common Criteria Part 2 Extended** and **Common Criteria Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.3 (Systematic flaw remediation).

Microsoft Windows Rights Management Services (RMS) 1.0 SP2 is an information protection technology that works with RMS-enabled applications to help safeguard digital information from unauthorized use—both online and offline, inside and outside a firewall. Using Windows Server 2003 features and security technologies, including encryption, certificates and authentication, RMS helps organizations create information protection solutions. RMS provides protection of information through persistent usage policies, which remain with the information, no matter where it goes.

The TOE is supported on Microsoft Windows Server 2003.

The 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 (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 4, augmented with Systematic Flaw Remediation (ALC_FLR.3) evaluation. Therefore the validation team concludes that the SAIC CCTL findings are accurate, and the conclusions justified.

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, 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 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:	Microsoft Windows Rights Management Services (RMS) 1.0 SP2
ST:	Microsoft Windows Rights Management Services (RMS) Security Target, Version 1.0, 9 July 2007
Evaluation Technical Report	Evaluation Technical Report for Microsoft Windows Rights Management Services (RMS) 1.0 SP2: • Part 1 (Non-Proprietary), Version 1.0, 9 July 2007 • Part 2 (Proprietary), Version 1.0, 9 July 2007
CC Version	Common Criteria for Information Technology Security Evaluation, Version 2.3
Interpretations	None
CEM Version	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004
Conformance Result	CC Part 2 extended, CC Part 3 conformant

Item	Identifier
Sponsor	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399
Developer	Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Rick Murphy, Noblis Jerry Myers, Aerospace

3 Security Policy

The Microsoft Windows Rights Management Services (RMS) 1.0 SP2 TOE enforces the following security policies as described in the Security Target.

> ***Note:*** *Much of the description of the RMS security policy has been extracted and reworked from the Microsoft Windows Rights Management Services (RMS) Security Target and Final ETR.*

3.1 Security Audit

The TOE has the ability to log Use License requests. When logging is enabled, all attempts to acquire Use Licenses are logged by forwarding them to the local SQL server configured in the IT environment of the TOE.

3.2 User Data Protection

The TOE ensures that certificates are generated with appropriate contents. The TOE also restricts the issuance of Use Licenses to content users who have been granted rights that would be reflected in a license issued by the TOE.

3.3 Identification and Authentication

While the TOE depends upon the IT environment to properly authenticate user identities, the TOE requires the identity of the applicable users before it can process requests for Client Licensor Certificates and Use Licenses.

3.4 Security Management

The TOE provides the administrator with functions to manage the audit function, Use License issuance controls and exclusion list, the decommissioning service, and dictating the applicable content of certificates and licenses.

4 Assumptions

The following assumptions underlying the evaluation of RMS are identified in the Microsoft Windows Rights Management Services (RMS) Security Target.

4.1 Usage Assumptions

Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.

Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

4.2 Physical Assumptions

The processing resources of the TOE are assumed to be located within controlled access facilities that will prevent unauthorized physical access.

The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

4.3 Personnel Assumptions

There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.

4.4 Clarification of Scope

The TOE does not store or control access to protected content. Instead, it generates certificates and licenses that can be used to encrypt content and enable access to those authorized to use the content. RMS provides the setup steps that enable trusted entities to use rights-protected information. The enforcement of protection on RMS-protected content is implemented by RMS-enabled applications, which are not included in the evaluation.

The TOE relies on the underlying operating system and its security. The operating system on which the TOE is installed is outside the TOE and hence its security properties are not covered by this evaluation.

The TOE is intended for use within a closed network environment that is not connected to the Internet. This restriction is made clear in the guidance documentation, as is the process for obtaining the root certification key via an external computer with Internet connectivity and a removable media device.

A number of product features are excluded from evaluation. A detailed listing of exclusions, and their rationale, is provided in the Security Target. In brief, they are:

- Lockboxes (RMS Activation Service)

  Lockboxes refer to the RMS client software. RMS client software is outside the TSC because it is implemented as a user mode client side library that is potentially by-passable.

- Pre-Licensing

  The concept of "pre-licensing" refers to the publisher requesting a Use License on behalf of another user at publishing time so that it can provide this end user with all the required licenses to consume a piece of content. This optional feature depends upon the RMS enabled client application. Since it is assumed that all users are authenticated by the IT Environment, this functionality would violate this assumption; hence it is outside the TOE. An RMS enabled client application that requests a Use License at publishing time is using an unevaluated capability of the TOE. The administrator is relied upon to ensure that such applications are not enabled as the TOE does not enforce restrictions against issuance of such licenses.

- Server certification

  Server certification provides a Rights Account Certificate for a server or service on a particular computer rather than an authenticated user. This optional feature is also known as "server lockbox"; it is not included in the TOE because it is assumed only authenticated users using desktop machines are consumers of RMS protected content. This capability is disabled in the evaluated configuration and administrators are instructed to not enable this capability.

- Mobile device certification

  Mobile device certification provides a Rights Account Certificate for RMS clients running Windows Mobile. This optional feature is not included in the TOE because the Windows Mobile platform is not conformant with the requirements for the IT environment. This capability is disabled in the evaluated configuration and administrators are instructed to not enable this capability.

- Temporary RACs

  Temporary RACs are intended for operating environments which offer anonymous or guest accounts; hence this capability is not included in the TOE. As with pre-licensing, a RMS enabled client application that requests temporary RACs is using an unevaluated capability of the TOE. The administrator is relied upon to ensure that such applications are not enabled.

- RACs based on .NET Passport credentials

  RACs based on .NET Passport credentials are outside the TOE because the mechanism used to authenticate .NET Passport credentials is not included in the evaluated configuration of the underlying IT environment.

- Group expansion across forests

  This functionality is not required because the IT Environment assumes a closed environment for a particular domain/forest when installing the RMS Server.

- Trusted domains

  The concept of "trusted domains" refers to other RMS installations that are trusted "user" and/or "publishing" sites. This optional feature is not included in the TOE because the IT Environment assumes a closed environment.

- Super users group

  The concept of a "super users" group is outside the TOE because it by-passes the RMS Use License Access Control Policy. This feature is disabled in the evaluated configuration and administrators are instructed to not enable this capability.

- Offline publishing (where an RMS-enabled client application issues a Publishing License)

  A publishing license created using the offline publishing model is outside the TOE because license creation is performed by the RMS client software which is outside the TSC.

- Re-Publishing

  The concept of "re-publishing" refers to modifying a Publishing License. This optional feature depends upon the RMS enabled application. It is outside the TOE because someone other than the RMS protected content's author is able to modify the Publishing License. This feature is disabled in the evaluated configuration and administrators are instructed to not enable this capability.

- Revocation lists

  Revocation lists are not included in the TOE because revocation is only enforced by the RMS client software which is outside the TSC.

5 Architectural Information

Note: *The following architectural description is based on the description presented in Part 1 of the Microsoft Windows Rights Management Services (RMS) 1.0 SP2 ETR and in the Security Target.*

The TOE comprises the following major subsystems:

- **Microsoft Hosted Services for RMS**

  This subsystem is hosted by Microsoft and provides the trust foundation for the RMS service. A deployed RMS Root Certification Server must receive a root Server Licensor Certificate from the Microsoft Host RMS Service, which contains the public key of the RMS Root Certification Server and is signed by the enrollment services of the Microsoft Hosted RMS Services.

Note that the RMS TOE must not have direct connectivity to external network environments, such as the Internet. In order to maintain an isolated environment for the evaluated configuration of RMS, an offline enrollment process is used. A root RMS Server Licensor Certificate request will be made from a computer that has Internet connectivity, but is maintained outside of the TOE. The certificate is then imported from removable media to the RMS TOE. The ability to make root RMS Server Licensor Certificate requests from an external computer and then import them into the root RMS server located on a separate network is a new feature that is available in the TOE.

- **RMS Root Certification Server**

  This subsystem provides the basis for managing RMS services within an organization. It maintains the chain of trust established by the Microsoft Hosted RMS Services and provides a mechanism for enrolling subordinate RMS Licensing Servers. The RMS Root Certification Server provides the capability for signing Publishing Licenses and generating Use Licenses for protected content. This subsystem also provides the capability for RMS Administrators to manage an organization's RMS implementation

  The RMS evaluation includes one RMS Root Certification Server per Active Directory forest. The IT environment for the RMS Root Certification Server comprises Windows Server 2003 SP2, hosting Internet Information Services (IIS) 6.0, Microsoft Message Queuing (MSMQ), ASP.NET 1.1, Internet Explorer 6.0, and Microsoft SQL Server 2005. In the evaluated configuration, IIS is configured to use SSL for the RMS Web site. The evaluated configuration does not include RMS Root Certification Server clustering configurations.

- **RMS Licensing Server**

  RMS Licensing Servers are enrolled RMS servers that are subordinate to the RMS Root Certification Server. These servers are a subset of the root server and provide the capability to sign Publishing Licenses and generate Use Licenses for valid consumers. RMS Licensing Servers are optional in the evaluated configuration and are deployed to relieve the workload from the RMS Root Certification Server.

  The IT environment for an RMS Licensing Server is the same as for the RMS Root Certification Server—Windows Server 2003 SP2 with: IIS 6.0, configured to use SSL; MSMQ; ASP.NET 1.1; Internet Explorer 6.0; and Microsoft SQL Server 2005 locally installed. The evaluated configuration does not include RMS Licensing server clustering configurations.

6 Documentation

The following documents are provided for use with the TOE. They are available for download from the following URL:

http://www.microsoft.com/technet/security/prodtech/windowsserver2003/ccc/default.mspx

The guidance documentation provides information pertinent to the installation, configuration, and operation of the TOE:

- Windows Rights Management Services (RMS) 1.0 with SP2 Evaluated Configuration Administrator's Guide, version 1.0, 9 July 2007
- Windows Rights Management Services (RMS) 1.0 with SP2 Security Configuration Guide, version 1.0, 9 July 2007
- Windows Rights Management Services (RMS) 1.0 with SP2 Evaluated Configuration User's Guide, version 1.0, 9 July 2007.

The above documentation was included within the scope of the evaluation. Any other documents downloaded from that web site are outside of the scope of the evaluation.

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 Report for Microsoft Windows Rights Management Services (RMS) 1.0 SP2, Version 1.0, 9 July 2007.

7.1 Developer Testing

The developer's approach to security testing for Rights Management Services is interface-based. Essentially, the developer has identified the security checks and effects related to each TSFI and has developed a test for each check and/or effect. These tests are organized into test families.

Each test family addresses both breadth and depth of coverage. Breadth is addressed by mapping all of the TSFI security checks and effects to a test case within a test family. Test depth is addressed by the descriptions of the test families. These descriptions explain algorithms, combinations, and sequence that are applied to each of the specific test variations that are identified by interfaces and associated properties (e.g., parameters). Together, these test families are designed to provide coverage of the security functions.

The developer produced five automated test suites and one manual (GUI) test suite. The developer ran the entire test suite on the test configuration described in the Test Plan and gave the evaluation team the actual results. The actual results comprise logs generated by the automated test suites and hand written results for the manual test suite. The test case reports identify that all tests passed. The evaluation team examined the test cases and determined that the expected behavior described at each test step would demonstrate the correct behavior of the TOE.

7.2 Evaluation Team Independent Testing

The evaluation team ran each of the test cases in the vendor's test suite to validate that the test cases correctly represent the behavior of the TOE and that the actual results match the expected results described in the test cases.

There are a number of test configurations that could be established to ensure that Windows Rights Management Services operates property. However, for the purpose of evaluation testing, a simple distributed architecture that consists of a Root Certification Server and one Subordinate Licensing Server was used. In addition, four other computers were configured to support the operating environment for the TOE. These computers are IT environment components outside the TOE. Specifically, one computer was configured as a Domain Controller and one computer was configured as a Certificate Authority to provide SSL certificates for IIS 6.0 RMS Web Sites. Finally, two computers were configured as RMS clients.

In general, the hardware is not important to the operation of the Root Certification Server or Licensing Server.

The test configuration comprised the following computers (the bolded roles are the roles performed by the TOE components):

Manufacturer	Model	Host Operating System	Role
HP	Proliant DL140	Windows Server 2003 SP2 x86 Enterprise	**RMS Root Certification Server**
HP	Proliant DL140	Windows Server 2003 SP2 x86 Enterprise	**RMS Licensing Server**
HP	Proliant DL140	Windows Server 2003 SP2 x86 Enterprise	Certificate Authority
Dell	Precision 670	Windows Server 2003 SP2 x64 Enterprise	Domain Controller
Dell	Precision 670	Windows XP Professional x64 SP2	RMS Client
Dell	Precision 670	Windows XP Professional x86 SP2	RMS Client

The computers supporting the RMS Root Certification Server and RMS Licensing Server are also configured with the following software in the supporting IT environment:

- Internet Information services (IIS) 6.0, configured to use SSL
- Internet Explorer 6.0
- ASP .NET 1.1.4322
- Microsoft Message Queuing (MSMQ)
- Microsoft SQL Server 2005.

Each of the RMS Client computers had RMS 1.0 SP2 Client software and Microsoft Office 2007 installed on them.

Another external computer, with Internet connectivity, was used to submit the request to the Microsoft-hosted Enrollment Service and download the enrollment response containing the Server Licensor Certificate during the installation and provisioning of the RMS Root Certification Server.

The evaluation team performed the following additional functional tests:

- Audit Generation: Test to ensure that all the required information is included in the audit records as a result of a Use License request. The evaluation team found that the description of the audit record provided in the ST and the guidance documentation did not match the structure of the audit record as viewed using SQL queries. The ST and guidance documentation was subsequently updated to provide the correct information

- License Generation: Test to ensure usage rights and symmetric content key included in the request must be encrypted with the server's public key and verified. By analysis, the evaluation team confirmed this is covered by the developer's testing
- Permission Enforcement: Test to demonstrate that an RMS-enabled application enforces the permissions set in a Use License by RMS. The evaluation team confirmed that a sample RMS-enabled application (in this case, Word 2007) correctly enforced permissions.
- Decommissioning: Test that the Decommissioning service issues content keys to any user enrolled in the RMS infrastructure, regardless of the content publishing license policy. The developer's test demonstrates the correct key is returned, but the evaluation team test showed that the use of this key is dependent on the RMS-enabled application (e.g., Word 2007 continues to enforce permissions after RMS has been decommissioned).
- Super Users Group: Test to ensure that no user (authorized or not) is part of the "Super Users Group" after RMS is installed.

The evaluation team performed the following vulnerability tests:

- IT Environment Controls: Ensure that NTFS permission do not bypass the RMS rights assigned to documents
- User Masquerade: Test to confirm a user cannot masquerade as a different user using another Rights Account Certificate (RAC).

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Microsoft Windows Rights Management Services (RMS) 1.0 SP2, running on Microsoft Windows Server 2003. To use the product in the evaluated configuration, the product must be installed and configured as specified in the following documentation:

- Windows Rights Management Services (RMS) 1.0 with SP2 Security Configuration Guide, version 1.0, 9 July 2007.

9 Results of the Evaluation

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 2.3 and CEM version 2.3 [1]–[4]. The evaluation determined the Microsoft Windows Rights Management Services (RMS) 1.0 SP2 TOE to be Part 2 extended, and to meet the requirements of Part 3 Evaluation Assurance Level 4 (EAL4), augmented with

ALC_FLR.3 (Systematic flaw remediation). The rationale supporting each CEM work unit verdict is recorded in the **Evaluation Technical Report for Microsoft Windows Rights Management Services (RMS) 1.0 SP2 Part 2** which is considered proprietary.

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 the vendor tests, the evaluation team's independent tests, and the penetration tests 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 user/integrator is cautioned that the evaluation makes several environmental assumptions about how the TOE is installed and used. The evaluated configuration assumes that the TOE is operated within a closed network, not connected to the Internet. This limitation may not be acceptable for some environments where the TOE might be used.

RMS has functionality that has not been evaluated. Unauthenticated operations such as "Use Licenses" and use of Temporary RACs (anonymous accounts) are not permitted but the TOE does not enforce this restriction, requiring that client applications be written to avoid unauthenticated operations and relying upon administrators to ensure that such applications are not used. In addition, there is TOE functionality documented in the Clarification of Scope section (4.4) of this document that is not normally enabled. If an administrator enables any of these capabilities, the TOE is no longer operating in the evaluated configuration. It is the responsibility of the administrator of the TOE to ensure that these capabilities are not enabled or used.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Microsoft Windows Rights Management Services (RMS) Security Target, Version 1.0, 9 July 2007.*

13 Abbreviations

The following abbreviations are used throughout this document:

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
NIAP	National Information Assurance Partnership
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
RAC	Rights Account Certificate
RMS	Rights Management Services
SAIC	Science Applications International Corporation
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSFI	TOE Security Function Interface

14 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is

complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

15 Bibliography

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

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 2.3, August 2005, CCMB-2005-08-001.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 2.3, August 2005, CCMB-2005-08-002.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 2.3, August 2005, CCMB-2005-08-003.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* –Evaluation Methodology, Version 2.3, August 2005, CCMB-2005-08-004.

[5] 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.

[6] Science Applications International Corporation. *Evaluation Technical Report for Microsoft Windows Rights Management Services (RMS) 1.0 SP2 Part 1*, Version 1.0, 9 July 2007.

[7] Science Applications International Corporation. *Evaluation Technical Report for Microsoft Windows Rights Management Services (RMS) 1.0 SP2 Part 2 (Microsoft Proprietary)*, Version 1.0, 9 July 2007.

[8] Science Applications International Corporation. *Evaluation Team Test Report for Microsoft Windows Rights Management Services (RMS) 1.0 SP2, ETR Part 2 Supplement (Microsoft Proprietary)*, Version 1.0, 9 July 2007.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[9] Science Applications International Corporation. *Microsoft Windows Rights Management Services (RMS) Security Target*, Version 1.0, 9 July 2007.