# National Information Assurance Partnership


# Common Criteria Evaluation and Validation Scheme Validation Report

## IBM Corporation, NY, USA

## IBM WebSphere Portal version 5.0.2

**Report Number: CCEVS-VR-04-0069**

**Dated: 23 August 2004**

**Version: 1.0**

**National Institute of Standards and Technology**
**Information Technology Laboratory**
**100 Bureau Drive**
**Gaithersburg, MD 20899**

**National Security Agency**
**Information Assurance Directorate**
**9800 Savage Road STE 6740**
**Fort George G. Meade, MD 20755-6740**

## ACKNOWLEDGEMENTS

### Validation Team

Donald Phillips, Lead Validator, Mitretek Systems

### Common Criteria Testing Laboratory

Science Applications International Corporation

Columbia, MD

## Table of Contents

# 1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of IBM WebSphere Portal version 5.0.2. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory, and was completed during August 2004. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by SAIC. The evaluation team determined the product to be **Part 2 conformant, Part 3 conformant,** and to meet the requirements of the **EAL2** assurance requirements**.**

IBM WebSphere Portal version 5.0.2 is a software application TOE that is provided within a set of products, which are:

- WebSphere Portal Enable;
- WebSphere Portal Extend;
- WebSphere Portal Express; and
- WebSphere Portal Express Plus.

During the evaluation, the evaluation team confirmed the vendor's claims that there is no reliance upon the underlying operating systems for the TOE to perform its security functions. The difference in the operating system has no bearing upon the TOE security functions. Therefore, the evaluation team concluded that the test configuration was a representative sample of the list included in the ST.

The Sponsor provided and the Evaluation team examined test results for the TOE installed upon the Windows 2000 and AIX platforms only. Test results of the TOE installed upon the other claimed Operating Systems stated in the Security Target were not evaluated in any capacity.

The TOE, IBM WebSphere Portal 5.0.2, allows authorized users to establish protected portal resources as defined in version 2.8 of the IBM Websphere Portal Security Target. As an example, authorized users can develop, share, and store information of the data types for web modules such as Portlet Application Definitions, Portlets, Content Nodes, User Groups, and URL Mapping contexts. This then allows for fast access to, and transfer of information between members of the team working on the same project.

When a user requests access to a resource from the web browser, WebSphere Portal relies upon WebSphere Application Server (WAS) to perform identification and management of users. The WebSphere Member Manager (WMM) is accessed to provide the group membership and a database for the mapping of users to roles and the actions to resources. The request is passed onto PAC.

Neither WAS or WMM are within the scope of the evaluation and are therefore considered part of the TOE IT Security Environment. WP also relies upon an OS and a database to operate however WP does not rely upon either the OS or database to provide any security functionality. The evaluation team verified this during the product testing activity. Also, the WebSphere Application Server (WAS) is currently undergoing a CCEVS evaluation for the EAL2 assurance requirements.

It is possible to configure WP to allow the access control functionality to be performed externally, however WP has no control over external applications within the environment and therefore this functionality is outside the scope of the evaluation.

The primary security features for the IBM WebSphere Portal version 5.0.2 are:

- **Access Control**: WebSphere Portal provides access control to protected resources such as Portlet Application Definitions, Portlets, Content Nodes, User Groups, and URL Mapping contexts. Access control is performed by the Portal Access Control (PAC) component with the WebSphere Portal TOE. Please note that the PAC is the only component within the TOE. The PAC is the single access control decision point within the WebSphere Portal (WP). It controls access to all sensitive portal resources. Protected resources are resources that can be accessed by a restricted set of users only. In order to be granted access to a protected resource in a specific way, the user needs a corresponding permission on this resource, e.g. a specific portal page can only be viewed by a specific user, if the user has the permission to perform the action 'View' on that page. The following types of resources are protected within the portal: Web Modules, Portlet Application Definitions, Portlets, Content Nodes (Pages), User Groups, URL Mapping contexts.

- **Security Management**: Users that have been assigned the role of Security Administrator or Administrator access to the Portal resource have the authority to grant or revoke access to all Portal resources. The TOE also allows Administrators the ability to delegate specific subsets of their administrative privileges to other users or groups. These users or groups can in turn delegate subsets of their privileges to additional users and groups. However, users that have been assigned the role of Security Administrator or Administrator with respect to a specific resource have the ability to grant or revoke access to only that resource. Access Control is supported by Security Management function.

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), 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 requirements and assurance requirements defined in the Security Target (ST) for an EAL2 evaluation. Therefore, the validation team concludes that the SAIC CCTL findings are accurate, 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 EAL 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 1: Evaluation Identifiers**

| Item | Identifier |
|---|---|
| Evaluation Scheme | United States NIAP Common Criteria Evaluation and Validation Scheme |
| Target of Evaluation | IBM WebSphere Portal version 5.0.2 |
| Protection Profile | Not applicable |
| Security Target | *IBM WebSphere Portal EAL2 Security Target, Version 2.8, dated 18 August 2004* |
| Evaluation Technical Report | *Evaluation Technical Report for IBM WebSphere Portal 5.0.2 ;* Version 0.5, dated August 6, 2004 |
| Conformance Result | CC Part 2 conformant, CC Part 3 conformant |
| Sponsor | IBM Corporation, NY, USA |
| Developer | IBM Corporation, NY, USA |
| Common Criteria Testing Lab (CCTL) | SAIC, Columbia, MD |
| CCEVS Validator(s) | Donald Phillips, Lead, Mitretek Systems |

# 3. ORGANISATIONAL SECURITY POLICY

The TOE must ensure that only those users with the correct authority are able to access a TOE resource on the basis of User membership of a group(s), User or Group(s) ID association with a role, Resource association with an Action set (and thus creation of a role); and actions assigned to the action set, and permission inheritance given by the protected resource hierarchy and role blocks. The TOE must also allow administrators of the TOE to effectively manage the TOE and that this is only performed by authorized users. The TOE also supports environmental objectives to further support the security policy. Those responsible for the TOE are assumed to be competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains. Those responsible for the TOE environment must ensure that each user on the supporting applications have associated User IDs and where applicable have an associated Group ID. Those responsible for the TOE environment must ensure that the supporting applications are installed and configured in accordance with the manufacturer's instructions, the evaluated configuration where applicable and is secure. Those responsible for the TOE environments must also ensure that procedures and/or mechanisms exist to ensure that data transferred between workstations is secured from disclosure, interruption or tampering. Lastly, those responsible for the TOE environment must ensure that procedures and/or mechanisms are provided to ensure that after system failure or other discontinuity, recovery without a security compromise is obtained.

# 4. ASSUMPTIONS

## 4.1 Personnel Assumptions

- There will be one or more competent individuals that are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, willfully negligent or hostile.

## 4.2 Physical Assumptions

- The applications that the TOE relies upon have been configured in accordance with the manufacturer's installation guides and where applicable, in its evaluated configuration. It is securely configured such that the applications protect the TOE from any unauthorized users or processes.

- All hardware, including network and peripheral devices, have been approved for the transmittal of protected data. Such items are to be physically protected against threats to the confidentiality and integrity of the data.

# 5. ARCHITECTURAL INFORMATION

PAC is the single access control decision point within WP. It controls access to all sensitive portal resources. Protected resources are resources that can be accessed by a restricted set of users only. In order to be granted access to a protected resource in a specific way, the user needs a corresponding

permission on this resource, e.g. a specific portal page can only be viewed by a specific user, if the user has the permission to perform the action 'View' on that page. The following types of resources are protected within the portal:

- Web Modules: Web modules are portlet archives that are installed on WAS. Web modules can contain multiple portlet applications. If a new Web module is installed, it is automatically a child of the Web Modules virtual resource;
- Portlet Application Definitions: Portlet applications provide a logical grouping of individual portlets. If a new Web module is installed, the portlet applications contained within that Web module are automatically child resources of the Portlet Applications virtual resource. Portlets contained within a portlet application appear as child nodes of that portlet application. A two-layer hierarchy consisting of portlet applications and the corresponding portlets exists beneath the Portlet Applications virtual resource;
- Portlets (Portlet Definitions): A portlet is an installed portlet having its own portlet configuration. E.g. a Mail portlet can be configured to a specific mail server
- Content Nodes (Pages): Pages (also known as content nodes) contain the content that determines the portal navigation hierarchy. A portal page is basically the frame that contains a specific set of individual portlets arranged in a specific layout. If a new top-level page is created, it is automatically a child resource of the Content Nodes virtual resource. If a new page is created beneath an existing page, the new page is automatically child of the existing page;
- User Groups: Users can be grouped into user groups (database records). User groups can be nested. Access privileges are propagated with user group's membership. If a new user group is created, it will appear as a corresponding child resource underneath the virtual resource User Groups.
- URL Mapping Contexts: URL mapping contexts are user-defined definitions of URL spaces that map to portal content. If a new top-level URL mapping context is created, it is automatically a child resource of the URL Mapping Contexts virtual resource. If a new URL mapping context is created beneath an existing context, the new context is automatically a child the existing context. URL mapping contexts inherit access control configuration from their parent context unless role blocks are used;

Users (database records) are implicitly protected resources, which means that access to specific user profile data can only be obtained via corresponding privileges on a user group that contains the given user as a member i.e. implicitly protected resources are those resources that are not linked into the protected resource hierarchy. Implicitly protected resources behave in the same was as normal protected resources. The Users virtual resource protects sensitive operations that deal with user management. For example, in order to add a user to a user group you must have the Security Administrator@Users role.

PAC directly supports access control configuration of hierarchical resource topologies through the concept of permission inheritance. This concept reduces the administration overhead for an

administrator when controlling access to a large number of portal resources. Inherited permissions are automatically assembled into roles that can be assigned to individual users and user groups, granting them access to whole sets of logically related portal resources. Permission inheritance can be prevented using role blocks. Role blocks can be either inheritance or propagation blocks, which prevent the inheritance of permissions from a parent resource, or propagation of the permissions to a child resource respectively.

Each of these resources has a database entry which contains a list of the roles that are authorized access to the resource. The access permissions are dependant upon those assigned to the role.

In addition to protected resources, portal access control supports the notion of virtual resources that are used to group resources of a specific type and to configure access to abstract concepts within the portal e.g. the virtual node portal provides a means to give a user full control over the portal. Access Control on the virtual resources behaves in the same way as non-virtual resources. The portal defines a set of fixed virtual resources, which are virtual resources that are created and initialized during portal installation.

Figure 1 shows the general layout of the resource topology that is protected by Portal Access Control. Figure 2 depicts an example sub-set of this topology that could exist in a real portal setup. Implicitly protected resources (light yellow boxes in Figure 1) are protected via their non-implicit parent resources. Thus, they do not need to show up in the PAC administration user interfaces. Implicitly protected resources are those resources that are not linked into the protected resource hierarchy.

It is possible to configure WP to allow the access control functionality to be performed externally, however WP has no control over external applications within the environment and therefore this functionality is outside the scope of the evaluation.

The PAC implementation is based on a layered architecture and supports two different kinds of flows: Access Control Administration Flows and Access Control Decision Flows. Access Control Administration Flows modify the access control configuration, for example, by creating a specific role assignment. Access Control Decision Flows do not modify the persistent data of PAC but provide high performance methods for checking individual permissions for specific principals (e.g. does Bob have the (view, SalesPage) permissions and retrieving entitlements information. Entitlements information comprises information about all the permissions a specific user has on a specific subset (e.g. all resources of a specific resource type) of the protected resource hierarchy.

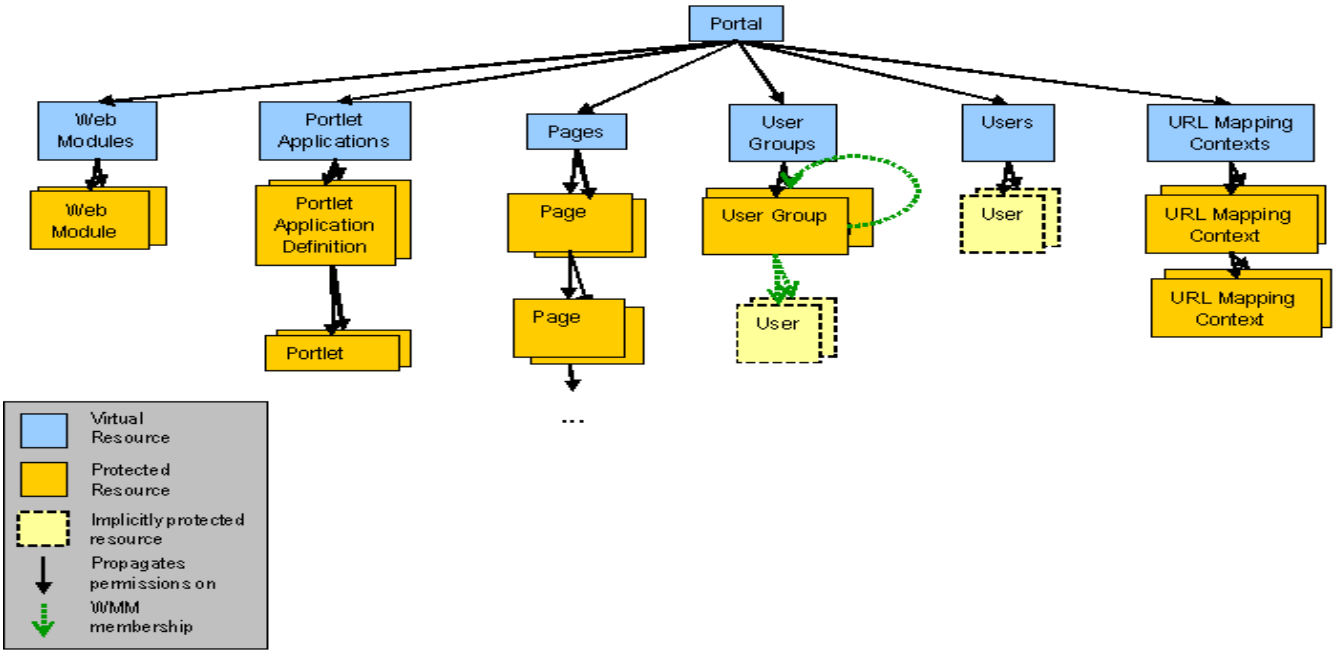


Figure 1

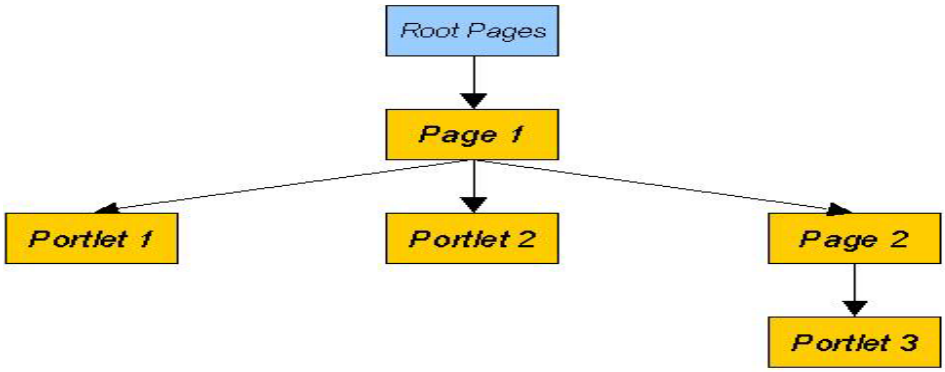


Figure 2

# 6. DOCUMENTATION

## Design documentation

| Document | Version | Date |
|---|---|---|
| WP5 Portal Access Control, System Design and Architecture Document, | Version 1.0.17 | 8 July 2004 |
| IBM Information Technology Security Standard | Version 204, 3.4 | |

| | | |
|---|---|---|
| IBM Information Technology Security Standard | Version 314, 1.0 | |

* Representation Correspondence Embedded in the Functional Specification and the High Level Design

## Guidance documentation

| Document | Version | Date |
|---|---|---|
| IBM WebSphere Portal for Multiplatforms Admin Guide | Version 5.0 | September 26, 2003 |
| IBM WebSphere Portal for Multiplatforms Overview Guide | Version 5.0 | September 26, 2003 |
| IBM WebSphere Portal for Multiplatforms Installation Guide | Version 5.0 | September 26, 2003 |
| Addendum to the System Administration Guide for Common Criteria | WP502/ADM/10 | July 15, 2004 |

## Configuration Management documentation

| Document | Version | Date |
|---|---|---|
| IBM WebSphere Portal EAL2 Configuration Management | Version 2.0 | March 5, 2004 |

## Delivery and Operation documentation

| Document | Version | Date |
|---|---|---|
| IBM WebSphere Portal EAL2 Delivery Documentation | Version 2.1 | May 7, 2004 |

## Test documentation

| Document | Version | Date |
|---|---|---|

| | | |
|---|---|---|
| IBM WebSphere Portal EAL2 Developer Testing | Version 2.4 | July 8, 2004 |

### Vulnerability Assessment documentation

| Document | Version | Date |
|---|---|---|
| IBM WebSphere Portal EAL2 Vulnerability Analysis | Version 1.0 | March 26, 2004 |

### Security Target

| Document | Version | Date |
|---|---|---|
| IBM WebSphere Portal EAL2 Security Target | Version 2.8 | 18 August 2004 |

# 7. IT PRODUCT TESTING

## 7.1 Developer Testing

IBM's approach to security testing for WebSphere Portal is security function based. Essentially, IBM developed a set of test suites that correspond to a security function. Each test suite targets the specific security behavior associated with that security function. The test procedures are designed to be exercised by running a script that has been designed to test the applicable security function described in the test scenarios.

Test coverage is addressed by analyzing the functionalities addressed in the functional specification and associating test cases that cover the addressed functionalities. Each security function is mapped to the appropriate test suite and the rationale demonstrates why the test suites cover that particular security function.

The vendor ran the entire test suite on the two identified platforms listed in section 7.2 below. The evaluation team performed the following analysis of the actual results produced by the vendor.

## 7.2Evaluator Testing

The evaluation team applied each EAL2 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 a complete test of the vendor's automated 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 following hardware is used to create the test configurations:*

*AIX:*

- *Any IBM machine that supports AIX V5.2 Power 32 bit only operating system.*
- *Physical memory: 1024 MB*
- *Typical disk space requirements are as follows:*
  - *Server installation: 1124 MB (on/usr)*
  - *Data storage: 50 MB (on/tmp)*

*Microsoft Windows:*

- *Any IBM PC machine (or compatible), based on a 32–bit Intel processor, that is year 2000 compliant and that is certified as Windows 2000 compatible.*
- *Physical memory: 1024 MB*
- *Typical disk space requirements are as follows:*
  - *Minimum of 1124 megabytes (MB) of disk space for Server installation and data*
  - *Minimum of 50 MB for working space.*
- *A suitable monitor for the operating system with a screen size of at least 800×600).*

*Operating Systems:*

- *Microsoft Windows 2000 (With Service Pack 2)*
- *AIX V5.2* with the following patch: AIX 5.2 APAR 43952

*Supporting Software:*

- WebSphere Application Server (WAS) 5.0;
- WebSphere Member Manager (WMM);

# 8. EVALUATED CONFIGURATION

The evaluation team determined the product to be **CC Part 2 conformant, CC Part 3 conformant,** and to meet the requirements of **EAL 2**. This implies that the product satisfies the security technical requirements specified in *WebSphere Portal EAL2 Security Target, dated18 August 2004.*

# 9. VALIDATOR COMMENTS

The IBM WebSphere Portal Security Target V2.8 makes a claim that the TOE can be supported on multiple Operating System Platforms. However, the full set of operating systems claimed in the ST was not all tested. During the evaluation, the evaluation team confirmed the vendor's claims that

there is no reliance upon the underlying operating systems for the TOE to perform its security functions. The difference in the operating system has no bearing upon the TOE security functions. Therefore, the evaluation team concluded that the test configuration was a representative sample of the list included in the ST.

The Sponsor provided and the Evaluation team examined test results for the TOE installed upon the Windows 2000 and AIX platforms only. Test results of the TOE installed upon the other claimed Operating Systems stated in the Security Target were not evaluated in any capacity.

The Validation team would also like to note that the Security Target V2.8 makes a claim in section 1.1.1 – 1.1.4 for four different packages that include the TOE (WebSphere Portal Enable, Portal Extend, Portal Express, Portal Express Plus). The packages all contain the same version of Portal (5.0.2), however only the WebSphere Portal Extend was tested.

# 10. SECURITY TARGET

The ST, IBM WebSphere Portal EAL2 version 2.8 dated 18 August 2004 is included here by reference.

# 11. GLOSSARY

| | |
|---|---|
| Authorised User | A user who may, in accordance with the TSP, perform an operation. |
| CC | Common Criteria |
| CCEVS | Common Criteria Evaluation and Validation Scheme |
| CCTL | Common Evaluation Testing Laboratory |
| CEM | Common Evaluation Methodology |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| IT | Information Technology |
| ITSEC | IT Security Evaluation Criteria |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards & Technology |
| NSA | National Security Agency |

| | |
|---|---|
| OS | Operating System |
| PAC | Portal Access Control |
| SF | Security Function. A part or parts of the TOE that have been relied upon for enforcing a closely related subset of rules from the TSP. |
| SFR | Security Functional Requirement |
| SOF | Strength of Function |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Function |
| TSP | TOE Security Policy. A set of rules that regulate how assets are managed, protected and distributed within the TOE. |
| WAS | WebSphere Application Server |
| WMM | WebSphere Member Manager |
| WP | WebSphere Portal |

# 12. BIBLIOGRAPHY


[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated August 1999, Version 2.1.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 1999, Version 2.1.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated August 1999, Version 2.1.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 1999, Version 2.1.

[5] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1998, version 0.6.

[6] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, version 1.0.

[7] Evaluation Technical Report for IBM WebSphere Portal v5.0.2

[8] WebSphere Portal EAL2 Security Target, Issue 2.8, 18 August 2004.

[9] NIAP Common Criteria Evaluation and Validation Scheme for IT Security, Guidance to Common Criteria Testing Laboratories, Version 1.0, March 20, 2001.

# 13. NATIONAL AND INTERNATIONAL INTERPRETATIONS

The evaluation team performed an analysis of the international interpretations and identified those that are applicable and had impact to the TOE evaluation. The table summarized the set of interpretations determined to have an impact on the evaluation and identifies the impact.

| Impact on Security Target Requirement | Impact on ETR Work Unit | Interpretation ID |
|---|---|---|
| New element added after ACM.CAP.4.3C | | RI #003 |
| ACM_SCP.2.1D and ACM_SCP.2.1C changed | | RI #004 |
| | ASE_DES.1.1C changed (no work unit change indicated) | RI #038 |
| | ASE_OBJ.1.2C and ASE_OBJ.1.3C changed (no work unit change indicated) | RI #043 |
| ADO_IGS.1.1C and AVA_VLA changed | | RI #051 |
| FMT_SMF, family addition to CC Part 2 | | RI #065 |
| | ASE_REQ.1-20 work unit changed | RI #084 |
| | ASE_REQ.1.10C (ASE_REQ.1-16 work unit changed) | RI #085 |
| FDP_ACF.1 modified | | RI #103 |