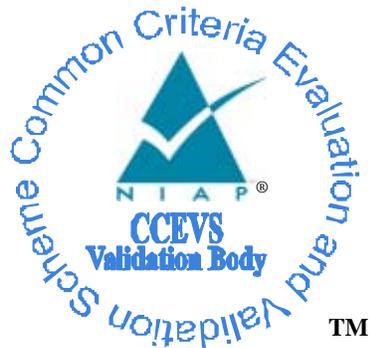# National Information Assurance Partnership

™

Common Criteria Evaluation and Validation Scheme Validation Report

BMC® Remedy® Action Request System® 6.3

Report Number: CCEVS-VR-07-0019
Dated: 10 April 2007
Version: 0.6

ACKNOWLEDGEMENTS

Table of Contents

List of Tables

1 Executive Summary

The evaluation of **BMC® Remedy® Action Request System® 6.3** was performed by SAIC, in the United States and was completed in March 2007. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the BMC Remedy AR System TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 2.3. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.3.

Science Applications International Corporation (SAIC) determined that the evaluation assurance level (EAL) for the product is EAL 3 family of assurance requirements. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the BMC® Remedy® Action Request System® 6.3 Security Target.

This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is a software-only product that relies on underlying operating system services as well as the services of a DBMS (for storage), LDAP server (for authentication), Web Server (to facilitate an alternate interface) and some other components within the execution environment of the TOE. It should be understood that the evaluation involved only the analysis of the TOE and its interactions with its environment, but did not include analysis of the operation of any of those components supporting the TOE. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of the BMC Remedy AR System by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation personnel monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation personnel 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 personnel 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 technical information included in this report was obtained from the Evaluation Technical Report For the BMC Remedy Action Request System Parts 1 and 2 and the associated test report produced by SAIC.

1.1 Evaluation Details

Evaluated Product: BMC® Remedy® Action Request System® 6.3:

- BMC® Remedy® Action Request System Server 6.3, patch 18

- BMC® Remedy® Approval Server 6.3 (no patch)

- BMC® Remedy® Email Engine 6.3, patch 18

- BMC® Remedy® Flashboards® Server 6.3 (no patch)

- Action Request System External Authentication LDAP Plug-in 6.3, patch 18

- BMC® Remedy® Mid Tier 6.3, patch 18

- BMC® Remedy® Administrator 6.3, patch 18

- BMC® Remedy® User 6.3, patch 18

- BMC® Remedy® Import 6.3, patch 18

- BMC® Remedy® Alert 6.3, patch 18

- BMC® Remedy® Configuration Tool 6.3, patch 18

Sponsor & Developer: BMC Software, Inc.
2101 City West Blvd.
Houston, Texas 77042

CCTL: Science Applications International Corporation
Common Criteria Testing Laboratory
7125 Columbia Gateway Drive, Suite 300
Columbia, MD 21046

Completion Date: March 2007

CC: Common Criteria for Information Technology Security Evaluation, Version 2.3

Interpretations: There were no applicable interpretations used for this evaluation.

CEM: Common Methodology for Information Technology Security Evaluation, Version 2.3

Evaluation Class: EAL 3

Description The BMC Remedy Action Request System (AR System) enables the secure automation of business processes, by enabling group based access controls on the applications and associated data.

Access to BMC Remedy AR System allows the administrator to set group-based permissions on various types of AR System controlled objects. This allows the administrator to control access at multiple levels, including applications and the components of applications, and data at the level of forms (tables), requests (rows) and fields (columns.) Groups further determine the type of operational access that group members have at each level, including view, modify, create, delete, execute, and no access. AR System server enforces access control at each level of access.

Disclaimer The information contained in this Validation Report is not an endorsement of the BMC Remedy AR System product by any agency of the U.S. Government and no warranty of the BMC Remedy AR System product is either expressed or implied.

PP:	none
Evaluation Personnel	Arnold, James
	Boone, John
Validation Personnel	Paul Bicknell
	Jean Hung

1.2 Interpretations

The Evaluation Team determined that there were no Interpretations applicable to this evaluation.

1.3 Threats to Security

The following are the threats that the evaluated product addresses:

Table 1 - Threats

T.UNAUTH_ACCESS	Unauthorized user	Access to TOE functions and data
T.EXCEED_PRIV	Unauthorized user	Access to protected user applications and data
T.MANAGE	Ability to manage	Adequacy of security management functions

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.

The following table serves to identify the evaluated Security Target and TOE:

Table 2 – ST and TOE identification

ST Title:	BMC® Remedy® Action Request System® 6.3 Security

TOE Identification:	• BMC® Remedy® Action Request System Server 6.3, patch 18
	• BMC® Remedy® Approval Server 6.3 (no patch)
	• BMC® Remedy® Email Engine 6.3, patch 18
	• BMC® Remedy® Flashboards® Server 6.3 (no patch)
	• Action Request System External Authentication LDAP Plug-in 6.3, patch 18
	• BMC® Remedy® Mid Tier 6.3, patch 18
	• BMC® Remedy® Administrator 6.3, patch 18
	• BMC® Remedy® User 6.3, patch 18
	• BMC® Remedy® Import 6.3, patch 18
	• BMC® Remedy® Alert 6.3, patch 18
	• BMC® Remedy® Configuration Tool 6.3, patch 18
CC Conformance:	• Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated August 2005, version 2.3, CCMB-2005-08-002
	• Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated August 2005, version 2.3, CCMB-2005-08-003
PP Conformance:	None
Assurance Level:	Evaluation Assurance Level 3
Operating Platform:	Windows and Solaris platforms as identified in the Security Target in conjunction with Oracle, SQL 2000, and Sybase ASE DBMS and Windows Server 2003 Active Directory and Sun One LDAP server, also identified in the Security Target

The first row of the table continues from a prior page: "Target, Version 4.5, March 28, 2007"

3   Security Policy

The Security Target identifies no organizational policies.

4   Assumptions

4.1   Physical Assumptions

The following physical assumptions are identified in the Security Target:

Table 3 – Personnel Assumptions

A.PEER_ASSOCIATION	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. This includes the network. (The network operates under the same constraints and resides within a single management domain.)
A.PHYSICAL_PROTECT	The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical access.
A.PLATFORM_SUPPORT	The underlying platform(s) upon which the TOE executes will provide reliable functionality including correct hardware operation and functionality, and correct platform software operation.

4.2 Personnel Assumptions

The following personnel assumptions are identified in the Security Target:

Table 4 – Physical Assumptions

A.INSTALL	The TOE software has been delivered, installed, and set up in accordance with documented delivery and installation/setup procedures and the evaluated configuration.
A.MANAGE	There will be one or more competent Authorized Administrators assigned to manage the TOE and the security functions it performs. Procedures will exist for granting Authorized Administrators access to the TSF.
A.NO_EVIL_ADM	An Authorized Administrator is not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the Administrator documentation.

4.3 Connectivity Assumptions

The following operational assumptions are identified in the Security Target:

Table 5 – Operational Assumptions

A.DAC	The host platform operating system of the TOE environment will provide discretionary access control (DAC) to protect TOE executables and TOE data.
A.DB_LOCKED_DOWN	The component database has had all current security patches (if applicable) applied, and the Authorized Administrator has configured the inherent database security mechanisms to their most restrictive settings that will still permit TOE functionality and interoperability. Any such patch does not interfere with the correct functioning of AR System server's interface to the database.
A.EXTERNAL_ AUTHENTICATION	The TOE environment will provide authentication mechanisms, as described in section 6.1.2 (of the Security Target), Table 12: Types of external authentication, and these mechanisms will function correctly and accurately.

A.TIME	The operating environment will provide reliable system time.
A.SECURE_ COMMUNICATION	The TOE IT environment will provide the ability to configure SSL communications where appropriate.
A.CONNECT	Any network resources used for communication between TOE components will be adequately protected from unauthorized access.

5   Architectural Information

The AR System consists of server and client components that can be combined to create the types of access the consumer wants to enable. Certain components are required for all AR System installations, while other components are optional, as indicated below. The TOE consists of all permutations of required and optional components described in this section.

The TOE does not include the hardware, database, operating systems, email servers, or directory service protocols with or on which the TOE components run, and also does not include third-party components of the mid tier, such as a web server, JSP servlet engine, or browser. However, these components are described in this section where required, to illustrate the physical scope and boundary of the TOE.

The AR System is built on a multi-tiered architecture (see Figure 1) that includes the server tier, the mid tier, and the client tier.

5.1   Server Tier

The server tier consists of AR System server, along with several optional *application servers* that provide specialized functionality, including Approval Server, Email Engine, and the Flashboards Server. These application servers provide commonly used services that administrators can incorporate into their customized applications, such as workflow approvals, automated notifications, and graphics that illustrate system status and history. If the Action Request System External Authentication (AREA) LDAP Plug-in *(AREA LDAP plug-in)* is used, it is also part of the server tier.

AR System server. The AR System server is a required component that is the core of the AR system. AR System server is a set of processes that run on the server host machine. It implements workflow and controls workflow logic, controls user access to the AR System and the database from AR System client applications, and controls the flow of AR System data into and out of the database. The AR System server installation also provides all APIs and server objects that make up the AR System, including forms, menus, active links, filters, and escalations.

AR System server can be installed on UNIX or Windows. The AR System server database abstraction layer makes the AR System database-independent, so it can operate with most

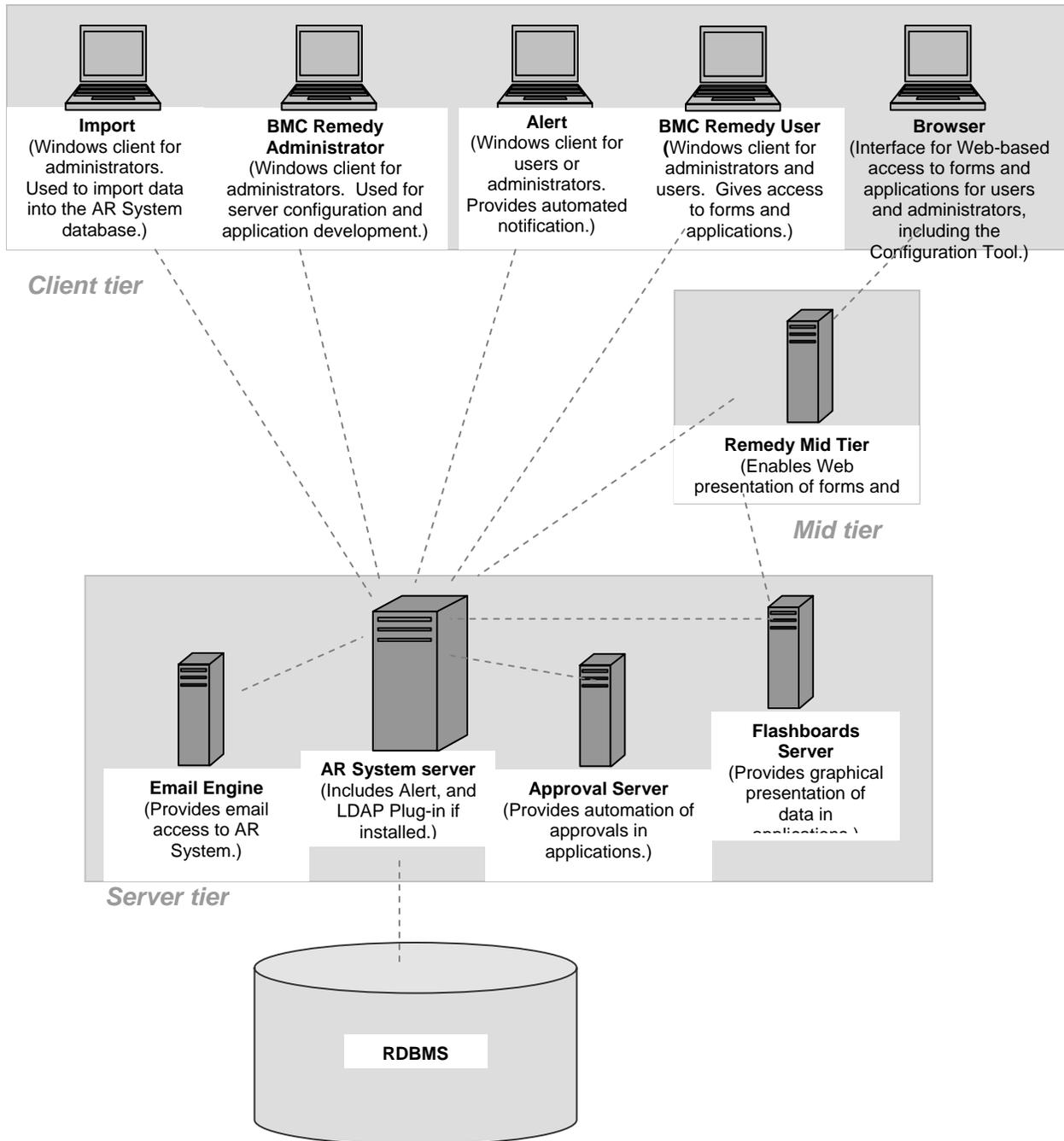popular databases, such as Oracle, Sybase, Informix, Microsoft SQL Server, and IBM DB2.

The server processes have no direct user interface. They communicate with AR System clients and the application servers through an application programming interface (API).

Figure 1: AR System multi-tiered architecture

Import
(Windows client for administrators. Used to import data into the AR System database.)

BMC Remedy Administrator
(Windows client for administrators. Used for server configuration and application development.)

Alert
(Windows client for users or administrators. Provides automated notification.)

BMC Remedy User (Windows client for administrators and users. Gives access to forms and applications.)

Browser
(Interface for Web-based access to forms and applications for users and administrators, including the Configuration Tool.)

Client tier

Remedy Mid Tier
(Enables Web presentation of forms and

Mid tier

Email Engine
(Provides email access to AR System.)

AR System server
(Includes Alert, and LDAP Plug-in if installed.)

Approval Server
(Provides automation of approvals in applications.)

Flashboards Server
(Provides graphical presentation of data in applications.)

Server tier

RDBMS

Approval server. The Approval Server is an optional application server component that adds approval functions to existing applications. This server provides a standard approach to adding an approval process to an AR System workflow application. This allows AR System developers to quickly and easily include approval functionality in applications, without having to develop their own approval system. It also allows them to implement a standard approach for approvals, so that AR System users do not have to figure out different approval mechanisms for each application. The Approval Server communicates directly with AR System server through the AR System API interface.

Email Engine. The Email Engine is an optional application server component that provides email access to AR System server, and is available for all supported platforms. The Email Engine enables applications to send notifications through email to users, and to have users submit AR System requests using an email client. This engine does not serve as an email exchange; it is simply an integration conduit between an email exchange server (like MS Exchange™, or UNIX mbox) and AR System. The Email Engine communicates directly with AR System server through the AR System API interface. It communicates with the email exchange server using IMAP4, SMTP, POP3, MAPI, or MBOX protocols. A supported Java SDK with JRE must be installed on the same platform as the Email Engine.

Only outgoing Email Engine functionality, for the purpose of sending notifications, is included in the evaluated configuration. Submission and modification of requests through the Email Engine is not included in the evaluated configuration.

Flashboards server. Flashboards is an optional application server component that consists of a server, forms, and GUI components. Flashboards provides graphics, such as pie charts and bar graphs, based on underlying AR System data. With Flashboards, the AR System administrator develops graphics within BMC Remedy AR System Administrator as part of an application. Users see color graphics as part of the user interface. These graphics pull data in real time from AR System server or from the *Flashboards server*, which in turn gets the data from the AR System server.

Flashboards forms and limited functionality are automatically installed with AR System server and their use is optional. Full functionality, including the use of flashboards that display historical data, requires licensing the Flashboards Server.

Flashboards requires Mid Tier to be installed. This is because the mid tier is used to construct the graphical presentation of the Flashboards graphics. The Flashboards Server communicates with AR System server through the AR System C API, and with the mid tier by means of the AR System Java API. The mid tier presents flashboards to the client in HTML format. The mid tier generates charts, converts them to HTML format, and then presents them to the client.

Alert. Alert consists of a server component and a client-side component. The server functionality for Alert is part of AR System server and is installed automatically with AR

System server. Alert can be configured to display the alert list in BMC Remedy User or in a browser.

Action Request System External Authentication (AREA) LDAP Plug-in. The AREA LDAP plug-in is an optional component that allows the administrator to configure external authentication by using the Lightweight Directory Access Protocol (LDAP). If configured, it accesses network directory services or other authentication services to verify the user login name and password. The AREA LDAP plug-in extends the AR System functionality to access directory services using the LDAP protocol.

To protect the password when the AREA LDAP plug-in is used, the administrator must configure the plug-in to use SSL.

A database. (The database is not included in the TOE.) A relational database is a required component of the IT environment. The database sits below the server tier and is accessed by AR System server only. It can be installed on any machine that is accessible to the AR System server.

The AR System server communicates with the database using the AR System database abstraction layer and the database API of the database in use.   At installation, the AR System server installer creates, or updates, an AR System database and a series of tables in the database that make up a data dictionary where form, filter, escalation, and other definitions are stored. The actual structure of the AR System database varies depending on the underlying relational database.

5.2   Mid Tier

Mid Tier. Mid Tier is optional middleware, installed on either UNIX or Windows, which works with a web server to enable AR System access through a web browser. The web server and Mid Tier can be installed on a separate machine with network access to the AR System server machine, or all can be installed on the same machine. One Mid Tier can permit access to multiple AR System servers, and one AR System server can be served by multiple Mid Tiers. Mid Tier communicates with AR System server through the AR System Java API interface.

Mid Tier also provides some administrator access to Mid Tier-related system management functions by way of the Configuration Tool, which runs in a browser. The following supporting components must be installed on the mid tier platform:

- **A supported web server. (The web server is not included in the TOE.)** Supported web servers include Apache, Websphere, Weblogic, SunONE, and IIS. Mid Tier communicates with the web server through the JSP engine.

  To protect the password when using a browser to access AR System, the administrator should configure the Web server to only allow https access.

- **A supported Java Server Pages (JSP) engine. (The JSP engine is not included in the TOE.) *For this evaluation ServletExec 5.0 was used.*** Mid Tier communicates with the JSP engine by means of JSP servlets.

- **Java SDK/JRE v1.4.2 or above. (The Java SDK is not included in the TOE.)** The Java SDK provides the runtime environment for the JSP servlets that make up Mid Tier.

The Configuration Tool. When the Mid Tier is installed, the administrator uses the Configuration Tool to configure the Mid Tier. The Configuration Tool is a .jsp script that is installed with Mid Tier. It does not access the AR System server. Rather, it forms a browser based interface to the Mid Tier configuration file, named config.properties. Administrators use the Configuration Tool to configure Mid Tier access to AR System servers and for other Mid Tier configuration settings. The Configuration Tool is accessed by entering the correct URL in a browser, and it requires a password to log in and change configuration settings.

The administrator must change the Configuration Tool password from the default to a unique password as soon as the Mid Tier installation is complete.

5.3   Client tier

The AR System client tier includes BMC Remedy Administrator, BMC Remedy User, Import, Alert, and, if Mid Tier is installed, a browser.

BMC Remedy Administrator. BMC Remedy Administrator is a required component. It is installed on Windows only, so at least one Windows client machine is required to administer and license any AR System server (UNIX or Windows). BMC Remedy Administrator is used to administer and configure AR System servers, and to develop AR System applications. One copy of BMC Remedy Administrator can be used to manage multiple AR System servers. It provides a graphical interface to the application's forms, fields, and workflow rules. Developers use BMC Remedy Administrator for application development. Administrators use it for managing the system, including some aspects of controlling security, as well as for customizing and changing BMC Remedy solutions. BMC Remedy Administrator communicates directly with AR System server through the AR System API interface.

BMC Remedy User. BMC Remedy User is a required component if Mid Tier is not installed. BMC Remedy User is installed on Windows and serves two functions. For administrators, it provides access to the User and Group forms that manage user access control, as well as access to other administrative forms. For users, it provides access to the AR System applications from client machines, to submit and modify requests and search the database. BMC Remedy User communicates directly with AR System server through the AR System API interface.

BMC Remedy User and BMC Remedy Administrator are both typically installed on client machines used by administrators. BMC Remedy User is also required for user access to the AR System in configurations that do not include Mid Tier. If Mid Tier is installed, then

BMC Remedy User is optional for user access to the AR System. The administrator can optionally configure the AR System to allow authorized administrators to manage the User and Group forms from a browser, if Mid Tier is installed.

Import. Import is installed with BMC Remedy Administrator. Import is an optional client tool that enables AR System administrators to transfer data from an external source into a database form. Import communicates directly with AR System server through the AR System API interface.

Alert. The Alert client is an optional component installed on Windows that provides notifications to users about new AR System transactions, such as when a ticket has been assigned to a user, when a ticket has been escalated, and so on. The purpose of the Alert client is to prompt the user by means of a sound, a window, or a flashing icon, to check the alert list in BMC Remedy User or in a browser.

A supported web browser. (The browser is not included in the TOE.) When Mid Tier is installed, a supported web browser must be installed on client workstations that will access the AR System through the mid tier. Supported web browsers include Internet Explorer, Netscape, and Mozilla. The browser communicates with the mid tier by means of http or https. *To protect the password when using a browser to access AR System, the administrator should configure the Web server to only allow https access.*

When the mid tier is installed, users can access AR System applications with a browser instead of BMC Remedy User. Web pages are written in JSP and rendered in JavaScript and HTML.

T*o secure the user password when using Mid Tier, the administrator should configure the web server to only allow https access.*

BMC supports AR System 6.3 compatibility with multiple operating system platforms, databases, and other third-party applications. To achieve a timely validation, BMC limited the IT Environment for Common Criteria testing to the platforms and third-party applications described in the *BMC Remedy Action Request System 6.3 Security Target*. For complete information about operating systems, databases, and other applications that are compatible with AR System 6.3, see the *AR System 6.3 Compatibility Matrix*, which is available at http://www.bmc.com/support_home.

6   Documentation

Following is a list of documents supplied by the developer for the TOE:

- BMC® Remedy® ActionRequestSystem® 6.3 Documentation Addendum, version 1.2, March 27, 2007
- Action Request System 6.3 Concepts Guide, January 2005, Part No:47832
- Action Request System 6.3 Installing AR System, January 2005, Part No:47838
- Action Request System 6.3 Configuring AR System, January 2005, Part No:47833
- Action Request System 6.3 C API Reference Guide, January 2005, Part No: 47829

- Action Request System 6.3 C API Quick Reference Guide, January 2005, Part No: 47830
- Action Request System 6.3 Developing AR System Applications: Basic, January 2005, Part No:47834
- Action Request System 6.3 Developing AR System Applications: Advanced, January 2005, Part No: 47835
- Action Request System 6.3 Remedy Email Engine Guide, January 2005, Part No:47836
- Action Request System 6.3 Database Reference Guide, January 2005, Part No:47889
- Action Request System 6.3 Error Messages Guide, January 2005, Part No:47837
- Action Request System 6.3 Optimizing and Troubleshooting AR System, January 2005, Part No:47891
- Remedy Approval Server 6.3 Guide for Users and Administrators, January 2005, Part No: 51329
- Action Request System 6.3 Remedy Flashboards Administrator's Guide, January 2005, Part No:49791
- Action Request System 6.3 Release Notes, February 6, 2006, Part No:47841

The security target used is:

- BMC® Remedy® Action Request System® 6.3 Security Target, version 4.5, 28 March 2007

7 IT Product Testing

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an EAL3 evaluation.

7.1 Developer Testing

Vendor testing is oriented toward security functional requirements as well as the various TOE components; the documentation includes a test plan describing test approach, test configuration, test procedures, and test coverage. Each test procedure is associated with a security functional requirement (SFR) and TOE component. The evaluation team found the vendor test suite to be sufficiently broad in scope, addressing each of the security functional requirements in combination with the related external interfaces.

7.2 Independent Testing

The evaluation team exercised all of the developer's manual test procedures, and developed some independent team tests to extend the developers tests.

The test configuration consisted of three TOE server (two with mid-tier instantiations) and a client instantiation, each configured per the defined evaluated configuration for the suite of BMC Remedy AR System applications. That is, the test configuration consisted of a single test environment, which included three TOE server and mid-tier instances:

- One running on Microsoft Windows Server 2003 with SQL Server 2000 and Active Directory

- One running on Sun Microsystems Solaris 9 with Oracle 9iR2 and Sun One 6.1
- One running on Sun Microsystems Solaris 9 with Sybase ASE 15.5.2 and Sun One 6.1

A client instance was established using Windows XP SP2 and another test client was set up for experimental purposes using Windows Server 2003.

An additional platform was required to host the following server products. These are not part of the TOE, but are in the IT Environment, and are required to execute the test scripts.

- Microsoft Exchange Server 2000

The evaluators installed the TOE according to the installation guidance and subsequently used the user and administrator guidance documents while performing tests.

Once the test configurations were established, the evaluator executed all of the developer's automated tests on each platform, in each case getting the expected results as documented by the developer.

Only a portion of the manual tests were executed on each configuration, given limited time available to test, though all of the tests were executed on at least one configuration. Between 55% and 85% of the manual tests were exercised on each configuration and the tests were selected such that at least some tests for each claimed security functions were exercised on each platform and to ensure coverage of all manual test procedures across all platforms. Given evaluation results demonstrating that the developer had run all the tests on the applicable configurations, the evaluators did not find it necessary to comprehensively exercise the available test procedures.

Of course, mid-tier tests were only run on the two configurations where the mid-tier was installed. The evaluation team had no reason to believe that the mid-tier should affect any tests nor behave differently between the two Solaris-based configurations. Executing tests with and without the mid-tier, except for the mid-tier tests, yielded no apparent difference in test results.

The evaluation team developed additional tests to extend the developer's testing for each of the claimed security functions and those tests are documented in the evaluation team test report.

8   Evaluated Configuration

The evaluated configuration is a single instance of the BMC Remedy AR System server and mid-tier as well as one or more BMC Remedy AR System client-tier applications that is comprised of the following components operating in the context of a Windows or Solaris operating system:

- BMC® Remedy® Action Request System Server 6.3, patch 18

- BMC® Remedy® Approval Server 6.3 (no patch)

- BMC® Remedy® Email Engine 6.3, patch 18

- BMC® Remedy® Flashboards® Server 6.3 (no patch)

- Action Request System External Authentication LDAP Plug-in 6.3, patch 18

- BMC® Remedy® Mid Tier 6.3, patch 18

- BMC® Remedy® Administrator 6.3, patch 18

- BMC® Remedy® User 6.3, patch 18

- BMC® Remedy® Import 6.3, patch 18

- BMC® Remedy® Alert 6.3, patch 18

- BMC® Remedy® Configuration Tool 6.3, patch 18

9   Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL3 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing Notes, Comments, or Vendor Actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes.

Section 5, Results of Evaluation, in the Evaluation Team's ETR, Part 1, states:

> The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR.

> 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 ([1], [2], and [3]) and CEM version 2.3 ([4]). The evaluation determined the BMC Remedy AR System TOE to be Part 2 conformant, and to meet the Part 3 Evaluation Assurance Level (EAL 3) requirements. The rationale supporting each CEM work unit verdict is recorded in the "Evaluation Technical Report For the BMC Remedy Action Request System Part 2" which is considered proprietary.

Section 6, Conclusions, in the Evaluation Team's ETR, Part 1, states:

> Section 6.1, ST Evaluation: Each verdict for each CEM work unit in the ASE ETR is a "PASS". Therefore, the BMC® Remedy® Action Request System® 6.3 Security Target, Version 4.5, March 28, 2007 is a CC compliant ST.

> Section 6.2, TOE Evaluation: The verdicts for each CEM work unit in the Proprietary part of the ETR are each "PASS". Therefore, when configured and operated according to the guidance documentation identified in section 6, above the BMC Remedy AR System TOE satisfies all of the security functional requirements stated in the BMC® Remedy® Action Request System® 6.3 Security Target, Version 4.5, March 28, 2007.

Additionally, the evaluation team's performance of a subset of the vendor test suite, the independent tests, and the penetration test also demonstrates the accuracy of the claims in the ST.

10   Validator Comments/Recommendations

The Validation personnel observed that the evaluation and all of its activities were performed in accordance with the CC, the CEM, and CCEVS practices. The Validation personnel agrees that the CCTL presented appropriate rationales to support the Results presented in Section 5 of the ETR and the Conclusions presented in Section 6 of the ETR.

The Validation personnel, therefore, concludes that the evaluation and Pass result for the TOE identified below is complete and correct:

BMC® Remedy® Action Request System® 6.3:

- BMC® Remedy® Action Request System Server 6.3, patch 18
- BMC® Remedy® Approval Server 6.3 (no patch)
- BMC® Remedy® Email Engine 6.3, patch 18
- BMC® Remedy® Flashboards® Server 6.3 (no patch)
- Action Request System External Authentication LDAP Plug-in 6.3, patch 18
- BMC® Remedy® Mid Tier 6.3, patch 18
- BMC® Remedy® Administrator 6.3, patch 18
- BMC® Remedy® User 6.3, patch 18
- BMC® Remedy® Import 6.3, patch 18
- BMC® Remedy® Alert 6.3, patch 18
- BMC® Remedy® Configuration Tool 6.3, patch 18

11   Annexes

Not applicable.

12   Security Target

BMC® Remedy® Action Request System® 6.3 Security Target, Version 4.5, March 28, 2007

13 Acronym List

API	– Application Programming Interface
AR	– Action Request
AREA	– Action Request System External Authentication
CC	– Common Criteria
CEM	– Common Evaluation Methodology
CCEVS	– Common Criteria Evaluation and Validation Scheme
CCTL	– Common Criteria Testing Laboratory
DBMS	– Database Management System
EAL	– Evaluation Assurance Level
ETR	– Evaluation Technical Report
HTML	– Hypertext Markup Language
IT	– Information Technology
JSP	– Java Server Pages
LDAP	– Lightweight Directory Access Protocol
NIAP	– National Information Assurance Partnership
SSL	– Secure Socket Layer
SAIC	– Science Applications International Corporation
SFR	– Security Functional Requirement
SQL	– Structured Query Language
ST	– Security Target
TOE	– Target of Evaluation

Bibliography

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

[1]   Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 2.3, August 2005, ISO/IEC 15408-2.

[2]   Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.3, August 2005, ISO/IEC 15408-2.

[3]   Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.3, August 2005, ISO/IEC 15408-2.

[4]   Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.3, August 2005, ISO/IEC 15408-2.

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