National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Software AG webMethods Business Process Management Suite 8.2 SP2

Report Number: CCEVS-VR- VID10483-2013
Dated: 19 December 2013
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

Mario Tinto

The Aerospace Corporation

Ken Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos, Inc.
Columbia, MD

Table of Contents

1 Executive Summary 1
1.1 Evaluation Details 2
1.2 Interpretations 3
1.3 Threats 4
1.4 Organizational Security Policies 4
2 Identification 4
3 Security Policy 4
3.1 Security Audit 4
3.2 Cryptographic Support 5
3.3 User Data Protection 5
3.4 Identification and Authentication 5
3.5 Security Management 5
3.6 Trusted Path/Channels 6
4 Assumptions 6
4.1 Clarification of Scope 6
5 Architectural Information 6
6 Documentation 8
7 Product Testing 8
7.1 Developer Testing 8
7.2 Evaluation Team Independent Testing 9
7.3 Penetration Testing 9
8 Evaluated Configuration 10
9 Results of the Evaluation 10
10 Validator Comments/Recommendations 11
11 Annexes 11
12 Security Target 11
13 Bibliography 11

List of Tables

Table 1: Evaluation Details..... 2

1 Executive Summary

The evaluation of Software AG webMethods Business Process Management Suite 8.2 SP2 was performed by Leidos, Inc., Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America and was completed in December 2013. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1. The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the product is Common Criteria Part 2 Conformant and Common Criteria Part 3 Conformant, and that the Evaluation Assurance Level (EAL) for the product is EAL2 augmented with ALC_FLR.1. The information in this Validation Report is largely derived from the Evaluation Technical Report (ETR) and associated test reports produced by the Leidos evaluation team. 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 webMethods Business Process Management Suite 8.2 SP2, which consists of Integration Server with Process Engine, webMethods Broker, My webMethods Server with Task Engine, and Designer. webMethods BPMS is part of the larger webMethods Product Suite. The BPMS product provides application services together with business process management (BPM) in a service-oriented architecture (SOA).

The TOE requires host platforms including operating systems, Java Development Kit (JDK), and relational database management system (RDBMS). A JDK includes the Java Runtime Environment (JRE), in which TOE components execute. Suitable combinations of operating system, JDK, and RDBMS are described in webMethods System Requirements 8.2 .While there are some restrictions on combinations, in general the TOE components run with the following operating systems, JDK, and RDBMS.

Operating systems:

- Windows Server 2003 Standard and Enterprise Edition (x86 and x86-64)
- Windows Server 2008 Standard and Enterprise Edition (x86 and x86-64)
- Windows Server 2008 R2 Standard and Enterprise Edition (x86-64)
- SUSE Linux Enterprise Server 11 SPx (x86 and x86-64)
- Red Hat Enterprise Linux Server 5.x (x86 and x86-64)
- Red Hat Enterprise Linux Server 6.x (x86-64)
- Solaris 10 (64 Ultra SPARC and x86-64)
- HP-UX 11i v3 (PA-RISC64 and IA64)
- AIX 6.1 (Power 64-bit)

JDK:

- Oracle Java 1.6.0_24 or later (Windows, Linux, Solaris)
- HP Java 1.6.0.09 or later (PA-RISC 64)
- HP Java 1.6.0.07 or later (IA64)
- IBM Java 1.6.0 SR9 or later (AIX)

- Oracle Java 1.7.0_13 or later (Windows, Linux, Solaris)

RDBMS

- Oracle 11g (R1 and R2)
- DB2 9.7 LUW
- SQL Server 2003 and 2008

The operational environment contains commodity PC and browsers for Integration Server Administrator and My webMethods. Support browsers are:

- Microsoft Internet Explorer 7.x and 8.x
- Mozilla Firefox 3.x

The TOE may use an LDAP Directory server in the operational environment.

The operational environment includes components provided by Software AG and installed with the TOE. These components are:

- Entrust Authority™ Security Toolkit 7.2 for the Java© Platform,
- OpenSSL FIPS Object Module, and
- Jetty web server.

The Integration Server and My webMethods Server TOE components rely on Entrust Authority™ Security Toolkit 7.2 for the Java® Platform for cryptographic functions it provides. This toolkit is a FIPS 140-2 validated cryptographic module (certificate #802). webMethods Broker relies on OpenSSL FIPS Object Module 1.2.3 for cryptographic functions (FIPS 140-2 certificate #1051). My webMethods Server relies on the Jetty web server to present the My webMethods graphical user interface. Integration Server uses a file system to maintain its user database as well as an Apache Derby to store non-security-relevant databases. In the evaluated configuration, Integration Server may be configured to use an external RDBMS in place of the embedded database server for the user database.

The product, when configured as specified in the guidance documentation, satisfies all of the security functional requirements stated in the Software AG webMethods Business Process Management Suite 8.2 SP2 Security Target.

1.1 Evaluation Details

Table 1: Evaluation Details

Evaluated Product:	Software AG webMethods Business Process Management Suite 8.2 SP2
Sponsor:	Software AG USA, Inc. 11700 Plaza America Drive, Suite 700 Reston, VA 20190
Developer:	Software AG USA, Inc. 11700 Plaza America Drive, Suite 700 Reston, VA 20190

CCTL:	Leidos, Inc. Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	December 19, 2013
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.
Interpretations:	None
CEM:	Common Methodology for Information Technology Security Evaluation, Part 2: Evaluation Methodology, Version 3.1, Revision 3, July 2009.
Evaluation Class:	EAL2 augmented with ALC_FLR.1
Description:	The webMethods Business Process Management Suite 8.2 SP2 (BPMS) produced by Software AG USA, Inc. webMethods BPMS unites business processing management and service-oriented architecture capabilities to provide a comprehensive set of fully integrated tools for automating and managing processes. The webMethods BPMS TOE security features include assuring identification of users, controlling access to services, and auditing of user activity.
Disclaimer:	The information contained in this Validation Report is not an endorsement of the Software AG webMethods Business Process Management Suite 8.2 SP2 product by any agency of the U.S. Government and no warranty of the product is either expressed or implied.
PP:	n/a
Evaluation Personnel:	Leidos, Inc. Eve Pierre Dawn Campbell Greg Beaver Kevin Micciche
Validation Body:	National Information Assurance Partnership CCEVS

1.2 Interpretations

Not applicable.

1.3 Threats

The ST identifies the following threats that the Target of Evaluation (TOE) and its operational environment are intended to counter:

- A user may view, read, or write business process information without permission using BPMS interfaces.
- A user may invoke a service, web page, or business process task without permission.
- A user may modify the BPMS or its configuration in order to access services or business process information without permission.
- A user may capture network traffic in order to observe or alter service invocation or business process information of another user.

1.4 Organizational Security Policies

The ST identifies the following organizational security policies that the TOE and its operational environment are intended to fulfill:

- A product that provides security functions must be capable of producing an audit trail of security-relevant events.

2 Identification

The evaluated product is **Software AG webMethods Business Process Management Suite 8.2 SP2**.

3 Security Policy

The TOE enforces the following security policies as described in the ST.

> ***Note:*** *Much of the description of the Software AG webMethods Business Process Management Suite 8.2 SP2 security policy has been derived from the Software AG webMethods Business Process Management Suite 8.2 SP2 Security Target and Final ETR.*

3.1 Security Audit

The TOE records security-relevant events in audit records. Integration Server, webMethods Broker, and My webMethods Server generate audit records, which are stored in distinct audit trails. Security-relevant events include TOE configuration changes made by administrators, business process changes made by business analysts and IT developers, and service access by users. The set of audited events is configurable. Each audit record contains information suitable for analysis including date and time of the event, type of event, responsible identity, and event outcome.

The TOE provides tools to select Integration Server's audit records by time or number of records and view the subset in chronological or reverse chronological order. The TOE limits access to these tools. The Integration Server stores the audit records in a database, which the operational environment protects.

The TOE webMethods Broker and My webMethods Server store their audit trails in local operating system files, which the operating system protects. The TOE relies on the operational environment (for example, using a text editor) for review of webMethods Broker and My

webMethods Server audit records. My webMethods Server also provides ability to view audit trails via its web interface.

In addition, the TOE relies on the operational environment for reliable time stamps.

3.2 Cryptographic Support

Integration Server built-in services include services to digitally sign documents and verify digital signatures and to encrypt and decrypt documents. Business analysts and IT developers can use the built-in cryptographic services to present end users with digital signature and secure hash functions. These services rely on the operational environment, specifically JDK cryptographic providers and cryptographic functions of the Entrust FIPS 140-2 validated cryptographic module. The JDK cryptographic providers implement World Wide Web Consortium (W3C) XML standards. The cryptographic module provides cryptographic algorithms (RSA, AES, and Triple DES). The built-in services use the operational environment to make the cryptography capabilities available for use with documents.

The TOE supports secure communication with users and between TOE components with TLS. The TOE configuration determines which ports require TLS. The TOE relies on the operational environment for key management and cryptographic functions, which are provided by the JDK (for example, TLS session establishment) and FIPS 140-2 validated cryptographic modules (for example, AES encryption and decryption). Cipher suites used by the TOE include Triple DES, AES, DSA, and RSA using common key sizes (192 bits, 128 to 256 bits, 1024 bits, and 1024 to 4096 bits, respectively).

By default, JDK limits cryptographic key sizes. The defaults can be changed with a jurisdiction policy file. In order to allow use of longer keys (for example, 256-bit AES), the JVM in the operational environment must have an unlimited strength jurisdiction policy file.

3.3 User Data Protection

The TOE provides services to end users and provides development tools to business analysts and IT developers. The TOE enforces policies to limit access to services, tools, information, and resource to authorized users. The policy can limit service requests based on group membership, location (that is, source IP address), and service requested. It can limit access to other resources based on user name, group membership, role membership, owner of the resource, and operation requested. Administrators can configure access control policies and user permissions. Business analysts and IT developers may set user permissions on a limited basis (for example, on resources they own).

3.4 Identification and Authentication

Both access control policy enforcement and security audit depend on assured identity of users. The TOE provides password-based authentication and supports cryptographic authentication. In addition, the TOE supports use of an external LDAP server for authentication. The TOE enforces password composition rules. The TOE associates security attributes with each authenticated user. These attributes may include user name, group membership, role membership, password, and X.509 public key certificate. The TOE authentication policy is configurable so that some services and operations would require authentication while others would not.

3.5 Security Management

The TOE uses roles to manage privileges. Several Integration Server, webMethods Broker, and My webMethods Server roles have privilege to manage security functions. Collectively, these roles are identified with the Authorized Administrator role defined in this ST. The TOE also uses roles to enforce its access control policy.

The TOE includes tools needed to manage its security functions and limits their use to Authorized Administrators. An Authorized Administrator can configure security audit, network port restrictions, user accounts, groups, roles, access control policy, and password policy rules.

3.6 Trusted Path/Channels

The TOE supports secure communication for service requests and responses. The TOE can be configured to use a FIPS 140-2 validated cryptographic module to present services through HTTPS and, for Integration Server, FTPS. In addition, the TOE can be configured to use TLS version 1.0 to protect communication among TOE components and between webMethods Broker and its clients. The TOE supports LDAPS (LDAP over TLS) for connections with LDAP directories in the operational environment. The TOE relies on the operational environment for secure communication with RDBMSs.

4 Assumptions

The ST identifies the following assumptions about the use of the product:

- Those responsible for the TOE are trusted to correctly configure and operate the TOE according to the instructions provided by the TOE documentation.
- The operational environment must provide key management and underlying cryptographic functions to support TOE cryptographic operations.
- There is no untrusted software on the servers hosting the TOE.
- The TOE is protected from physical attack.
- The operational environment must provide text processing tools to supplement the TOE capability to review the security audit trail.
- Users will protect authentication data in their possession.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 augmented with ALC_FLR.1 in this case).
2. This evaluation only covers the specific version identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

5 Architectural Information

The TOE is a distributed application. Figure 1 shows the general network architecture for webMethods BPMS. One or more Integration Server(s) presents services to users. One or more Integration Servers provide access to enterprise resources. Business analysts and IT developers

develop services and business processes with Designer. Users perform business process tasks through My webMethods. Administrators manage a deployment, including security, through Integration Server Administrator and My webMethods graphical user interfaces. One or more webMethods Brokers provides messaging between the Integration Servers and My webMethods Server.

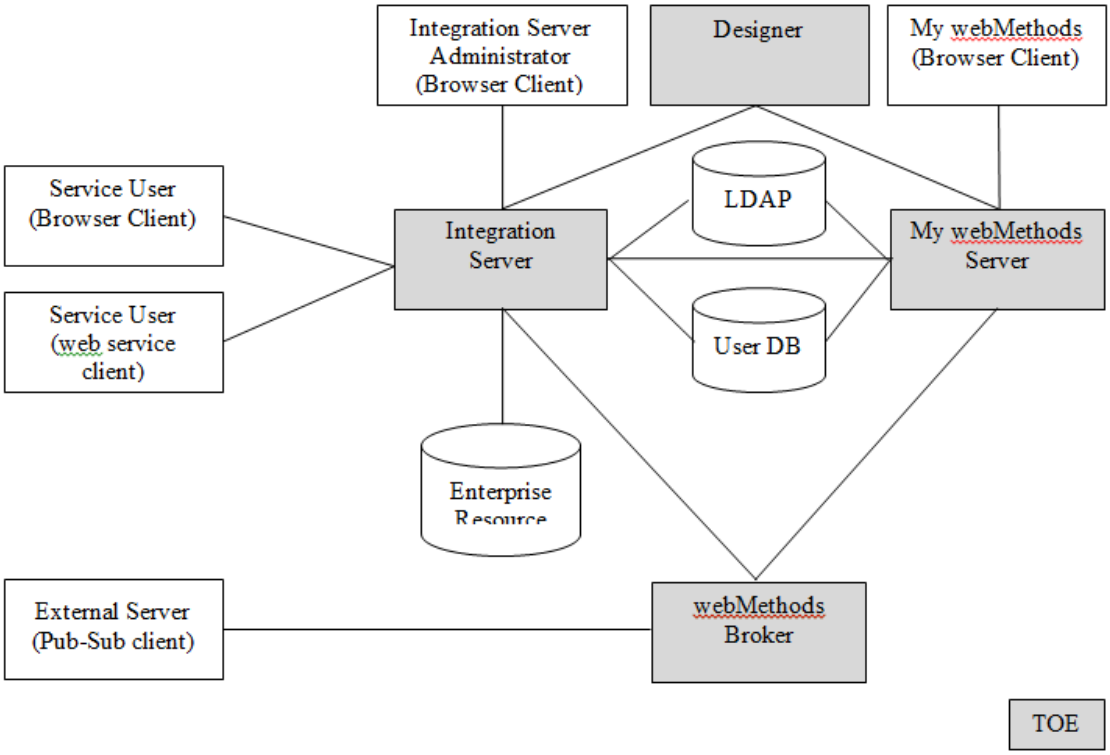

Figure 1: TOE Boundary and Components

Organizations deploy webMethods BPMS in a variety of operational environments. In some deployments, the operational environment strictly controls access by untrusted users to TOE components (for example, with firewalls) and protects communication between TOE components (for example, through isolated networks). In other deployments, internal users (for example, users performing tasks through My webMethods) may work on the same internal network as TOE components.

Consequently, the evaluated configuration includes a range of deployments. Some restrictions apply in all deployments. The TOE would be configured to protect its external interfaces. The TOE relies on the operational environment to restrict network access from public networks (for example, the Internet) to the TOE. The operational environment would be configured to protect TOE resources stored in the environment (that is, TOE executables and TOE data) as well the resources the TOE relies upon (that is, cryptographic modules, JVMs, LDAP server, RDBMS server, and application server).

In an environment where TOE communication and intra-TOE interfaces are visible to untrusted users (that is, end users, external servers, and non-administrative My webMethods users), the TOE would be configured to protect TOE communication (including management sessions from Integration Server Administrator and My webMethods Server) and intra-TOE interfaces. The TOE would be configured to use cryptographic functions of the operational environment to protect communication between TOE components from disclosure and undetected modification.

TOE components and the environment would be configured to protect communication between the components and the browsers and servers the TOE uses in the operational environment (for example, LDAP and RDBMS servers). In addition, each instance of webMethods Broker would be configured to authenticate all clients.

In an operational environment where TOE communication and intra-TOE interfaces are not visible to untrusted users, the TOE may rely on the operational environment for protection. TOE network communication may be in plain text where the operational environment prevents modification and disclosure. webMethods Broker need not authenticate clients, since no unauthorized clients would have access to Broker interfaces.

6 Documentation

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

Software AG offers a series of documents that describe the installation of webMethods BPMS as well as guidance for subsequent use and administration of the applicable security features.

- Using the Software AG Installer
- Understanding the webMethods Product Suite
- Working with My webMethods
- Installing webMethods Products
- Administering Integration Server
- Integration Server Build-In Services Reference
- Dynamic Server Pages and Output Template Developer's Guide
- Publish-Subscribe Developer's Guide
- Web Services Developer's Guide
- Administering Process Engine
- Working with BPM Tasks
- Administering webMethods Broker

TOE guidance documents are available from the Software AG documentation web site (http://documentation.softwareag.com/).

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Software AG Common Criteria Evaluator Test Procedures.

Testing took place in November 2013 at the Software AG facility in Reston Virginia. Vendor test engineers attended the testing and assisted the evaluation team in establishing and configuring the test environment to be equivalent to the test environment at the vendor testing site, and also in running vendor tests.

7.1 Developer Testing

The developer testing is comprised of both automated testing and manual testing. The vendor automated tests were created to fully exercise all of the functionality of the TOE and to exercise

the security features for every change made to the TOE. These automated vendor tests are ran on a nightly basis to ensure that any code changes made throughout the day by the development team have the correct functionality and that the changes have not broken or impacted the product in a negative manner.

Four of the automated tests that had a direct impact on the security functionality were repeated during evaluator testing. These tests include the following:

- The venusCerts test suite does full testing of all client and server usages of x.509 certificates.
- The venusAccess test verifys user/group/ACL testing. The test exercises the add/delete/modify users, groups, password restrictions, and ACLs.
- The venusTriggerEnhancements trigger access control checks session management, and broker configuration.
- The venusScheduler schedules tasks and ACL testing for scheduled tasks.

The developer also included manual tests that were targeted specifically targeted for Common Criteria testing. The evaluator repeated the four manual tests to exercise user management, ACLs, and testing the management and use of X.509 certificates.

7.2 Evaluation Team Independent Testing

The evaluation team executed the developer test suite per the evaluated configuration as described in the Software AG webMethods Business Process Management Suite 8.2 SP2 Security Target.

The tests were run at the developer facility with the configuration identified in the Security Target.

The actual test environment established at the developer location for evaluation team testing comprised:

- Integration Server installed on a Red Hat Enterprise Linux Server 5
- webMethods Broker installed on a Red Hat Enterprise Linux Server 5
- My webMethods Server installed on a Windows Server 2008
- Designer installed on a Window 7 computer

The evaluation team devised and performed additional functional test activities covering:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- TSF Protection
- Inter-TSF Trusted Channel

7.3 Penetration Testing

The evaluation team performed a search of public vulnerability databases. No vulnerabilities were identified as a result of the open source vulnerability searches. The following vulnerability tests were executed:

- Open Source Search
- Unsupported Protocols Scan and Ports Scan
- Web Vulnerability Scan
- User Input Validation
- User Account Harvesting
- Security Patch Verification

8 Evaluated Configuration

The evaluated version of the TOE is Software AG webMethods Business Process Management Suite 8.2 SP2.

The TOE is webMethods Business Process Management Suite 8.2 SP2 (BPMS) produced by Software AG USA, Inc. webMethods BPMS unites business processing management and service-oriented architecture capabilities to provide a comprehensive set of fully integrated tools for automating and managing processes. The webMethods BPMS TOE security features include assuring identification of users, controlling access to services, and auditing of user activity.

9 Results of the Evaluation

The evaluation was conducted based upon version 3.1 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL2 augmented with ALC_FLR.1" certificate rating be issued for Software AG webMethods Business Process Management Suite 8.2 SP2.

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

TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_ARC.1	Security architecture description
ADV_FSP.2	Security-enforcing functional specification
ADV_TDS.1	Basic design
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.2	Use of a CM system
ALC_CMS.2	Parts of the TOE CM coverage

Assurance Component ID	Assurance Component Name
ALC_DEL.1	Delivery procedures
ALC_FLR.1	Basic flaw remediation
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing - sample
AVA_VAN.2	Vulnerability analysis

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Software AG webMethods Business Process Management Suite 8.2 SP20 meets the claims stated in the Security Target.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality, such as Web Services security, included in the product was not assessed as part of this evaluation.

The devices were evaluated at EAL2 augmented with ALC_FLR.1, and the results of those evaluations reviewed via the VOR process which provided the testing laboratory and vendor with additional observations regarding the content and format of the test results. The testing laboratory and vendor made every effort to incorporate those changes to the documents and testing associated with this product.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is Software AG webMethods Business Process Management Suite 8.2 SP2 Security Target, Version 0.6, 11/08/13.

13 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 3, 2009.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1, Revision 3, July 2009.
4. Common Methodology for Information Technology Security: Evaluation Methodology, Version 3.1, Revision 3, July 2009.
5. Software AG webMethods Business Process Management Suite 8.2 SP2 Security Target, Version 0.6, 11/08/13.