Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0659-2011

for

SAP NetWeaver Application Server Java
7.02 SP3 with Common Criteria Addendum
(material no. 51039496)

from

SAP AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0659-2011

Java Application Server

SAP NetWeaver Application Server Java
7.02 SP3 with Common Criteria Addendum (material no. 51039496)

from	SAP AG
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1

Common Criteria
Recognition
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 8 February 2011

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalski L.S.
Head of Department

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement.

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product SAP NetWeaver Application Server Java 7.02 SP3 with Common Criteria Addendum (material no. 51039496) has undergone the certification procedure at BSI.

The evaluation of the product SAP NetWeaver Application Server Java 7.02 SP3 with Common Criteria Addendum (material no. 51039496) was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 2 February 2011. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: SAP AG.

The product was developed by: SAP AG.

[6] Information Technology Security Evaluation Facility

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product SAP NetWeaver Application Server Java 7.02 SP3 with Common Criteria Addendum (material no. 51039496) has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] SAP AG
Dietmar-Hopp-Allee 16
69190 Walldorf

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1 Executive Summary

The Target of Evaluation (TOE) defined as SAP NetWeaver Application Server Java 7.02 SP3 with Common Criteria Addendum (material no. 51039496) (in the following also called NWAS Java or NWAS Java 7.02) consists solely of software (accompanied by the associated guidance documentation). This software application represents a fundamental component used in modern SAP systems.

As an application server, the TOE represents a framework for the development and execution of Java applications based on the J2EE software architecture. The TOE provides a complex set of services and infrastructure to be used by such applications.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.2. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
Security Audit	The TOE maintains a security log to keep track of security relevant events. It further provides functionality for review of the audit to authorized administrators.
Users and Authorization	The TOE provides two different concepts for access control: Declarative Security: Within the declarative security concept for access control applications inform the TOE about the required permissions for users to access an object under access control. Every time the application requests access to an object under control (on behalf of a user) the TOE verifies the permissions of that user and denies the access to the object in case that the user does not have the required permission. Programmatic Security: In an application using the programmatic access control concept the application itself forms an important part of the overall policy. The TOE provides the application with services to acquire the (confirmed) identity of the user and to check whether the current user has the requested permissions. However, it falls into the responsibility of the application to deny user access to resources in case that the user does not have the appropriate permissions.
Identification and Authentication	In order to provide access control the TOE has to be aware of the identity of the connection user. Therefore the TOE provides an identification and authentication function based on usernames and passwords. The identification of subjects can be used for attaching authorizations to these subjects and allows access control decisions based on a subject's identity and authorizations.
Security Management	The focus of this security functionality is to provide only authorized administrators with the functionality to manage all relevant aspects of the security functionality of the TOE.

Table 1: TOE Security Functionality

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. Based on these assets the TOE Security Problem Definition is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapters 3.3, 3.4 and 3.5.

For the configuration of the TOE covered by this certification please refer to chapter 8 of this report.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

SAP NetWeaver Application Server Java
7.02 SP3 with Common Criteria Addendum (material no. 51039496)

The following table outlines the product deliverables:

No	Type	Identifier	Version	Form of Delivery
1	SW	SAP NetWeaver Application Server Java	7.02 SP3 with Common Criteria Addendum (material no. 51039496)	Physically via DVD-ROM
2	DOC (Guidance part)	TOE documentation SAP Library [10]	7.02 SP3 with Common Criteria Addendum (material no. 51039496)	
3	DATA	Hash files (SHA-1) shafile.dat (stored on the DVDs)	7.02 SP3 with Common Criteria Addendum (material no. 51039496)	
4	DOC (Guidance part)	NWAS Java 7.02 Guidance Addendum (File name: NWAS_EAL4_AGD_A DD_0 97.pdf) [9]	0.97 File size: 2.357.558 Bytes SHA-1 hash value: 49A4813ADEA60AEFCCB 87C3C20C8D1AD2B3041 97	Download (via SSL-secured SAP Common Criteria website) [11]
5	DATA	Hash values (SHA-1) for the shafile.dat hash files	N/A	Published on SSL-secured SAP Common Criteria website [11]
6	SW	Java Development Kit (JDK)	1.4.2_25 Rev b02, platform ‘Windows x64’	Download (via SUN JDK download website) [12]
7	SW	Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.4.2	1.4.2	

No	Type	Identifier	Version	Form of Delivery
8	DATA	Hash value (SHA-1) for the JDK	N/A	Published on SSL-secured SAP Common Criteria website [11]
9	DATA	Hash value (SHA-1) for the Java(TM) Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.4.2		
10	SW	SHAValidator	1.01	Download via SSL-secured SAP website [13]

Table 2: Deliverables of the product

The TOE (No. 1-4, software accompanied by guidance documentation) is delivered partly via physical distribution on a set of DVDs (comprising 5 DVDs) and partly (particularly the guidance addendum) via download from dedicated website [11]. Additional components (No. 5-10, e.g. integrity check tool, files and data) are part of the delivery process as they are required for the TOE integrity check process.

The TOE label is displayed to the consumer in various forms during the delivery and operational phase of the TOE. In detail, the TOE can be identified by the following methods referring to the placement of label as well as the kind of label (e.g. electronically, engraved, printed, etc.):

- Service Marketplace (SAP internet portal for software delivery) [14]: TOE referenced by its reference label SAP NetWeaver Application Server Java 7.02 SP3 with Common Criteria Addendum (material no. 51039496).
- Delivery media (DVD set with the TOE installation media): TOE referenced as SAP EHP2 FOR SAP NETWEAVER 7.0. The DVD set shipped physically is equipped with a label, i.e. the installation basis DVDs include the identifier ‘SAP EHP2 FOR SAP NETWEAVER 7.0’, while the Common Criteria Addendum DVD includes the identifier ‘Common Criteria Addendum – SAP NetWeaver Application Server Java 7.02 SP03’. It should be noted that the reference ‘SAP EHP2 FOR SAP NETWEAVER 7.0’ is equivalent to the identification ‘SAP NetWeaver Application Server Java 7.02‘, since the information ‘EHP2 for 7.0’ corresponds one-to-one to the product release ‘7.02’. After installation of the installation basis DVDs and the Common Criteria Addendum DVD (material no. 51039496) the complete TOE SAP NetWeaver Application Server Java Release 7.02 SP3 with Common Criteria Addendum (material no. 51039496) is build. This DVD labelling facilitates the TOE identification for consumers at the point of receipt of the DVDs.
- Operational TOE: In the running TOE, several status info screens are available containing the version info of the underlying NWAS, see [9] chapter 3.4.

Both parts of the guidance documentation (consisting of TOE documentation and Guidance Addendum) include a unique reference see table 2, so that it is possible to identify them uniquely. In addition, table 2 contains the SHA-1 checksum for NWAS Java 7.02 Guidance Addendum in order to enable customers to verify the correctness of the guidance document obtained.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Security Audit
- Users and Authorization
- Identification and Authentication
- Security Management

For more information on these issues, see Security Target [6], chapter 3.5.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target are not covered by the TOE itself. These assumptions lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- The administrator of the TOE shall be non hostile and well trained.
- The administrator of the TOE shall know and follow all instructions provided in the relevant guidance documentation.
- It has to be ensured that the emergency user account “SAP*” is not used in the operational use of the TOE.
- Authentication data for each user account for the TOE is kept securely and not disclosed to persons not authorized to use that account.
- Administrators and users must specifically ensure that no hardware or software key loggers are installed on the machines used to enter the authentication data.
- The TOE is connected to the Internet and/or terminals and workstations.
- Authentication and authorization data transported between client and server data is protected and the TOE is appropriately protected by a firewall.
- An appropriate hardware architecture and a suitable operating system shall be available.
- The runtime environment shall supply a reliable clock for the TOE's usage.
- The TOE and its underlying abstract machine are used in a controlled environment.
- It has to be ensured that the TOE is used with suitable user interfaces as set out in the TOE guidance documents.
- It has to be ensured that the development of applications for the TOE will comply with all the guidelines and restrictions specified in [9].

Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The following Figure 1 provides a graphical overview of the TOE architecture with consideration of the subsystems:

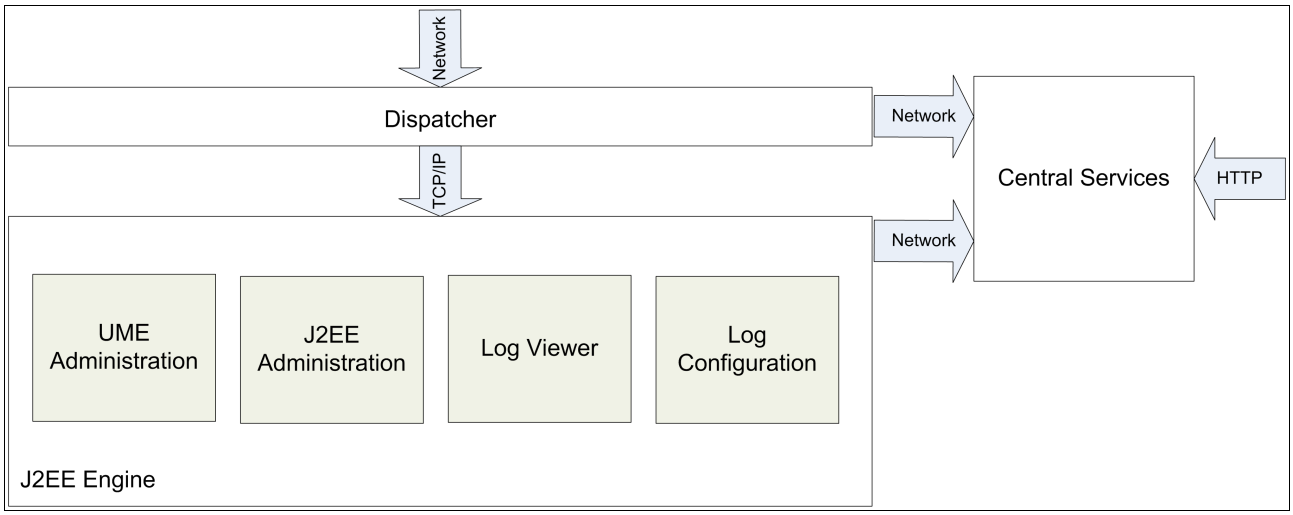

Figure 1: TOE architecture

The TOE consists of the following subsystems:

Subsystem	Description
Dispatcher	● Realizes network access to TOE ● Hands on network connections to the J2EE Engine server process(es)
J2EE Engine	● Provides the infrastructure for J2EE applications that consist of EJB modules (business logic) and Web modules (presentation logic) ● Allows the modules to communicate with each other and controls access of callers to applications
UME Administration Application	● Used by authorized users to administer the TOE (except management of J2EE roles)
J2EE Administration Application	● Used by authorized users to administer the J2EE roles
Log Viewer Application	● Used by authorized users to view TOE logs
Log Configuration Application	● Used by authorized users to configure TOE logs
Central Services	● Provides communication services via the Message Server and synchronization services via the Enqueue Server ● Message Server informs all the servers (instances) belonging to an SAP System of the existence of the other servers ● Enqueue Server implements the lock management for data objects stored in the database

Table 3: TOE design

6 Documentation

The evaluated documentation as outlined in table 2 (No. 2 and 4) is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7 IT Product Testing

7.1 Developer Testing

TOE Test Configuration

All developer's tests in the context of the evaluation have been conducted using the final version of the TOE. Independently on whether manual or automatic tests were performed the following software configuration was in place:

- Operating System: Microsoft Windows Server 2008, Enterprise Edition (x64)
- Additional Software: JDK Version 1.4.2_25 Rev b02 (for platform 'Windows x64')

The developer used different hardware for automated and manual testing as stated below:

- The hardware used for the automatic tests is an Intel Xeon E5504 2GHZ CPU based PC with 8 GB RAM and 464 GB hard disk space.
- The hardware used for the manual tests is a virtual machine running Windows Server 2008 Enterprise Edition (x64) on a 2.6 GHz AMD Opteron Processor. The machine is configured with 8GB RAM and 120 GB disk space and is hosted by VMWare ESX v3.5 U5 Build 213532 on a HP ProLiant DL585D2. The JDK used is Sun 1.4.2_25-rev-b02 x64, and the DB used is SAP DB (a.k.a. MaxDB), version 7.8.01.

Testing Approach

The developer used four different test tools for different aspects of the testing activities, e.g for managing manual and automated test cases.

Conclusion

The developer has tested the TOE systematically at the level of TSFI as well as at the level of subsystems. The tests results demonstrate that no discrepancy between the TOE behaviour and the TOE specification has been found.

7.2 Evaluator Independent Testing

TOE Test Configuration

1. Repetition of developer tests:
   - NWAS Java 7.02 installed on Microsoft Windows Server 2008 Enterprise Edition x64 running on an x64 CPU. The TOE uses the MaxDB database delivered on the TOE installation DVDs and the Sun JDK version as specified in the Guidance Addendum which are installed on the same machine as the TOE.
   - The hardware used for the repetition of the developer tests is an Intel Xeon E5504 2GHZ CPU based PC with 8 GB RAM and 464 GB hard disk space.

2. Evaluation body's own testing:
   NWAS Java 7.02 installed according to [9] on:
   - Hardware: HP ProLiant ML330 G6 Server, 8GB RAM, Dual Core, 2 GHz
   - Operating System: Microsoft Windows Server 2008 Enterprise (x64)

Testing Approach

The evaluator repeated all automatic developer tests, thereby covering all TSFI. The evaluator further developed a set of own manual test cases for independent testing. Thereby he had chosen the approach to cover TSF from all the functional areas of the TOE (Audit, Identification and Authentication, Users and Authorization and Security Management). This approach extends the one used for the repetition of the developer tests, so that both TSF and TSFI coverage is given.

The following TSFI where used for testing of SFR-relevant behaviour during evaluation body testing:

- Dispatcher Network Interface
- J2EE API
- SAP API
- UME Admin App
- J2EE Admin App
- Log Configuration Tool
- Log Viewer Tool

Conclusion

The overall test result is that no deviations were found between the expected and the actual test results, i.e. all test cases have passed.

7.3 Evaluator Penetration Testing

TOE Test Configuration

The penetration testing was performed using the evaluation body's testing environment:

- Operation System: Microsoft Windows Server 2008 Enterprise (x64)
- Hardware: HP ProLiant ML330 G6 Server, 8GB RAM, Dual Core, 2 GHz

Testing Approach

The evaluator analysed the development and guidance documentation from an attacker's perspective to find security flaws in design and implementation of the TOE. In addition to that he applied security scanners to find common vulnerabilities in web applications and used a static code analysis tool to detect programming errors in TOE functionality that could lead to security vulnerabilities.

Furthermore, publicly known vulnerabilities were searched on the internet and considered for penetration testing.

The following list summarizes areas considered for vulnerability testing:

- Common vulnerabilities in web applications were searched
- A port scan has been conducted to identify attack vectors

- It was examined whether the TOE is vulnerable against common vulnerabilities by using a sophisticated security scanner
- Static code analysis has been performed on the source code of the TOE in order to identify security relevant programming errors
- Possible TOE specific vulnerabilities have been addressed by dedicated tests

Conclusion

No deviations were found between the expected and the actual test results. No attack scenario with the attack potential enhanced-basic was actually successful in the TOE's operational environment as defined in the Security Target [6].

8 Evaluated Configuration

The TOE under evaluation is SAP NetWeaver Application Server Java 7.02 SP3 with Common Criteria Addendum (material no. 51039496). The Security Target [6] has identified solely one configuration (NWAS Java single stack mode installation) of the TOE under evaluation. This configuration is achieved by strict adherence of the Guidance Addendum. The TOE as specified in the Security Target [6] is set up as a single system, i.e. its environment does not connect to other SAP systems or application servers.

The operational environment of the TOE in its evaluated configuration can be summarized as follows:

- Software requirements:
  - TOE platform (OS): Microsoft Windows Server 2008 Enterprise Edition (x64),
  - supported Database management system
  - Java Development Kit (JDK), 1.4.2_25 Rev b02, platform 'Windows x64'
- Hardware requirements (minimum characteristics):
  - CPU: 1.4 GHz (x64 processor)
  - RAM: 5 GB
  - Hard disk: 64 GB,
  - Others: Super VGA (800×600) resolution monitor, DVD-ROM drive, Keyboard and Microsoft Mouse (or compatible pointing device), Internet access.

For the certified configuration of the TOE the following patches have to be installed:

Vendor/Name	Target Release SPLevel PatchLevel
sap.com/CORE-TOOLS	7.02.3.7
sap.com/JLOGVIEW	7.02.3.2
sap.com/LM-TOOLS	7.02.3.4
sap.com/SAP-JEE	7.02.3.8
sap.com/SAP-JEECOR	7.02.3.15
sap.com/SAP_JTECHF	7.02.3.4

Vendor/Name	Target Release SPLevel PatchLevel
sap.com/SAP_JTECHS	7.02.3.11

Table 4: Patches

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None
- For the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant
- For the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.1

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

The TOE does not include cryptoalgorithms. Thus, no such mechanisms were part of the assessment.

10 Obligations and Notes for the Usage of the TOE

The operational guidance documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of assumptions as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE shall be used. If non-certified updates or patches are available he should request the sponsor for providing a re-certification. In the

meantime the risk management process of the system using the TOE shall investigate and decide on the usage of not yet certified updates and patches or to take additional measures in order to maintain system security.

In addition, the following aspects need to be fulfilled when using the TOE:

- The emergency user ('super admin user') account "SAP*" that is provided by the system (and disabled by default) shall not be used in the operational phase of the TOE.
- The customer is required to verify the integrity of all relevant guidance documentation using SHA-1 checksums and comparing those against the values provided in table 2.

11 Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12 Definitions

12.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
DB	Database
EAL	Evaluation Assurance Level
EJB	Enterprise Java Beans
ETR	Evaluation Technical Report
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
J2EE	Java 2 Platform, Enterprise Edition
JCL	Java Class Library
JDK	Java Development Kit
NWAS	NetWeaver Application Server
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement

SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interfaces
UME	User Management Engine
VGA	Video Graphics Array

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Authenticated user - This subject belongs to a user of the operational functions (e.g. HR, FI) of an SAP system who has gone through a logon process and is thus identified and authenticated.

Authentication - Verifying the claimed identity of a user.

Authentication Data - information used to verify the claimed identity of a user

Authorization - The authority to execute a particular action in the SAP System. Each authorization references an authorization object and defines one or more permissible values for each authorization field contained in the authorization object.

Authorized User - TOE user who may, in accordance with the SFRs, perform an operation

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8]

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-0659-2011, Version 1.16, 2010-12-20, Security Target NWAS Java, SAP AG

[7] Evaluation Technical Report, Version 4, 2011-02-02, Evaluation Technical Report Summary, TÜViT (confidential document)

[8] Configuration list for the TOE (confidential document):

[Clist_Perforce] Configuration List from Perforce, SAP AG, Version 1.0, 2010-12-20, List of SAP Perforce files for 'SAP NetWeaver Application Server Java 7.02 SP3 with Common Criteria Addendum (material no. 51039496)'
[Clist_Java-Code_DTR] Configuration List from DTR, SAP AG, Version 1.1, 2010-12-23, List of SAP DTR files for 'SAP NetWeaver Application Server Java 7.02 SP3 with Common Criteria Addendum (material no. 51039496)
[Clist_KW] Configuration List from Knowledge Warehouse, SAP AG, Version 1.0, 2010-12-17, List of SAP KW files for 'SAP NetWeaver Application Server Java 7.02 SP3 with Common Criteria Addendum (material no. 51039496)'
[BOM] Bill of Material, SAP AG, Materialnumber: 52026088, 2011-01-25, BOM: SAP NW 7.0 EHP2 Java Common Criteria
[Ref] Reference List, SAP AG, Version 1.6, 2011-01-25, NWAS Java 7.02 Reference-List
[Bug_List] List of security flaws, Version 1.0, 2010-11-15, List of all security bugs for NWAS Java 7.02

[8] specifically

- AIS 1, Version 13, 14. August 2008, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 11, Version 2, 02. Februar 1998, Programmiersprachen und Compiler
- AIS 14, Version 7, 03. August 2010, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 8, 19. Oktober 2010, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria) und ITSEC
- AIS 23, Version 2, 11. März 2009, Zusammentragen von Nachweisen der Entwickler
- AIS 32, Version 6, 03. August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 41, Version 1, 20. August 2008, Guidelines for PPs and STs

[9] Guidance documentation for the TOE, SAP AG, Version 0.97, 20. December 2010, NWAS Java 7.02 Guidance Addendum

[10] Guidance documentation for the TOE, SAP AG, Version 7.02, 2010-04, SAP Product documentation

[11] SAP Common Criteria website, https://service.sap.com/commoncriteria

[12] SUN JDK download website, http://java.sun.com/j2se/1.4.2/SAPsite/download.html

[13] SAP Notes, https://service.sap.com/notes

[14] SAP Service Marketplace, https://service.sap.com

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-

Assurance Class	Assurance Components
	level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.”

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0659-2011

Evaluation results regarding development and production environment

The IT product SAP NetWeaver Application Server Java 7.02 SP3 with Common Criteria Addendum (material no. 51039496) (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 8 February 2011, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_FLR.1, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

a) SAP AG, Dietmar-Hopp-Allee 16, 69190 Walldorf; Germany (Development)

b) SAP AG, Raiffeisenring 45, 68789 St.Leon-Rot, Germany (Development and Production)

c) SAP Labs Israel, 15 Ha'tidhhar St', 43665 Ra'anana, Israel (Development)

d) SAP Labs Bulgaria, Бул.”Цар Борис” III 136 A, 1618 Sofia, Bulgaria (Development)

e) SAP Labs India Pvt. Ltd., #138, EPIP Zone Whitefield Bangalore – 560066, India (Development)

f) SAP Moscow, Представительство SAP AG в, России Moskau, Russia 115054 г.Москва Космодамианская наб., 52/2 (Development)

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.