Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0909-2015

for

**JBoss Enterprise Application Platform 6,
Version 6.2.2**

from

Red Hat, Inc.

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-0909-2015

Server Applications: Application Servers

JBoss Enterprise Application Platform 6
Version 6.2.2

from	Red Hat, Inc.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3
Valid Until:	12 April 2020

SOGIS
Recognition Agreement

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 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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.

(*) For details on the validity see Certification Report part A chapter 4.

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.

Common Criteria
Recognition Arrangement

Bonn, 13 April 2015
For the Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bernd Kowalski
Head of Department

L.S.

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:

- Act on the Federal Office for Information Security[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 ISO/IEC 17065 standard
- BSI certification: Technical information on the IT security certification, Procedural Description (BSI 7138) [3]
- BSI certification: Requirements regarding the Evaluation Facility (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- 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 EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels Technical Domains have been defined. They include assurance levels

[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

beyond EAL 4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: 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 by the nations listed above.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. for all assurance components selected.

As this certificate is a re-certification of a certificate issued according to CCRA-2000 this certificate is recognized according to the rules of CCRA-2000, i.e. for all assurance components selected.

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 JBoss Enterprise Application Platform 6, Version 6.2.2 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0687-2011. Specific results from the evaluation process BSI-DSZ-CC-0687-2011 were re-used.

The evaluation of the product JBoss Enterprise Application Platform 6, Version 6.2.2 was conducted by atsec information security GmbH. The evaluation was completed on 12 February 2015. atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Red Hat, Inc.

The product was developed by: Red Hat, Inc.

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, as 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 order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited as outlined on the certificate.

The owner of the certificate is obliged

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report and the Security Target and user guidance documentation mentioned herein to any applicant of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,

[6] Information Technology Security Evaluation Facility

3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the product's evaluated life cycle, e.g. related to development and production sites or processes, occur or the confidentiality of documentation and information related to the product or resulting from the evaluation and certification procedure is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the product or resulting from the evaluation and certification procedure that do not belong to the product deliverables according to the Certification Report part B chapter 2 to third parties, permission of the Certification Body at BSI has to be obtained.
4. to provide latest at of half of the certificate's validity period unsolicitedly and at his own expense current qualified evidence to the Certification Body at BSI that demonstrates that the requirements as outlined in the Security Target are up-to-date and remain valid in view of the respective status of technology. In general, this evidence is provided in the form of a re-assessment report according to the rules of the BSI Certification Scheme.

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 JBoss Enterprise Application Platform 6, Version 6.2.2 has been included in the BSI list of 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] Red Hat, Inc.
Varsity Drive
NC 27606 Raleigh

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) is the JBoss Enterprise Application Platform 6, Version Version 6.2.2, which implements an application server. JBoss is based on Java Enterprise Edition (Java EE) and therefore supports a large variety of operating systems. As an application server, JBoss allows client computers or devices to access applications. Access to these applications is possible through different network protocols, such as HTTP and RMI-IIOP. JBoss handles the business logic of the applications, including accessing and providing the user data required by the 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.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
Access Control	Using access control, the TOE is able to restrict access for the following request types with the following access control mechanisms: • HTTP: URLs and paths provided with URLs can be protected from access by subjects. • EJB: EJBs and associated method names can be protected from being called by subjects. • HornetQ: Message queue destinations and topic destinations can be protected from access by subjects.
Role-based access control for management interfaces	The management interfaces of JBoss, the command line interface as well as the web-based administrative interface, allow access to the JBoss system configuration to manage all configurable aspects of JBoss EAP. A set of pre-defined roles is shipped with the TOE and is available after installation (Monitor, Configurator, Operator, Administrator, Deployer and Auditor).
Audit	The TOE implements an audit mechanism that allows generating audit records for security-relevant events concerning access control. The administrative user is able to select the events which are to be audited.
Clustering	Clustering allows the execution of applications on several parallel servers (a.k.a cluster nodes). Two different cluster concepts are possible with JBoss: a failover cluster and a load-distribution cluster. In both cases, the server state is distributed across different servers, and even if any of the servers fails, the application is still accessible via other cluster nodes.
Identification and authentication	Users are assigned unique user identifiers which are used as the basis for access control decisions and auditing. The TOE authenticates the claimed identity of the user before allowing the user to perform any further TSF-mediated actions. The TOE internally maintains the

TOE Security Functionality	Addressed issue
	identifier associated with the thread spawned for the user after a successful authentication.
Transaction Rollback	JBoss includes a fast in-VM implementation of a JBoss Transactions compatible transaction manager that is used as the default transaction manager. A transaction is defined as a unit of work containing one or more operations involving one or more shared resources having ACID properties. ACID is an acronym for atomicity, consistency, isolation and durability, the four important properties of transactions.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configurations of the TOE as outlined in chapter 8.

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:

JBoss Enterprise Application Platform 6, Version 6.2.2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	Archive or Image	jboss-eap-6.2.0.zip (apply patch 6.2 CP02) SHA256: 627773f1 798623eb 599bbf7d 39567f60 941a706d c971c17f 5232ffad 028bc6f4 jboss-eap-6.2.0-installer.jar (apply patch 6.2 CP02) SHA256: 26ce5f13 948167b9 bb7b9ce5 bf59402f 9c5b27d5 7ade3457 463349ef 5057d9bb jboss-eap-6.2.2.zip (Patch 6.2 CP02) SHA256: 94f2ec3a 1a741646 90252959 c9afb378 2b3c1ea8 84c43643 c683ed74 dcf891ba jboss-eap-6.2.2-cc.zip SHA256: 9414619e 186708b3 4381ddbe f1901a51 335b5b45 464838ef fb153b61 0b27918f jboss-eap-6.2.2-cc-rhel-5-noarch.iso SHA256: d1424bb3 32d15f1f 239cc758 1379751b 9089a772 56a25c06 ff8972f5 666a9f62 jboss-eap-6.2.2-cc-rhel-6-noarch.iso SHA256: b48ae2f1 43e79d73 eb00c6eb 20625b6a 04085f97 c7137df4 d0766ba5 55493177	Version 6.2.2	Electronic delivery via Red Hat Network or Customer Service Portal
2	DOC	Red Hat JBoss Enterprise Application Platform Common Criteria Certification 6.2.2 Common Criteria Configuration Guide [8] SHA256: 1f2e5d20 ef793c31 394f1f7e 5e49ca44 306a63cd 49b97a32 a2c48fec 4447cf56	Version 6.2.2, 2014-06-24	
3	DOC	JBoss API JavaDoc [9]	Version JBoss EAP 6.2.2, 2014-03-31	
4	DOC	JBoss Enterprise Application Platform Common Criteria Certification 6.2 Installation Guide [10]	Version 2.0-23, 2014-02-14	
5	DOC	JBoss Enterprise Application Platform 6.2 Administration and Configuration Guide [11]	Version 6.2, 2014-03-10	
6	DOC	JBoss Enterprise Application Platform 6.2 Development Guide [12]	Version 6.2, 2014	
7	DOC	HornetQ User Manual [13]	Version 2.3, 2012	
8	DOC	Red Hat JBoss Enterprise Application Platform Common Criteria Certification 6.2.2 Security Guide [14] SHA256: dc934d19 e39c46bf cd079ad7 b3bc33a2 a22482c8 6f460d58 bd8705ac 464cfb17	Version 6.2.2-14, 2014-05-21	

Table 2: Deliverables of the TOE

The TOE is made up of components distributed as RPM packages, which are compiled into an ISO image for easy retrieval at Red Hat Network (RHN) or as zip files available on both RHN and the Customer Portal (CP). The distinction between the two delivery methods is simply dependent on the chosen customer's operating system. In other words, customers who use Linux (i.e., JBoss EAP subscribers) can pick the RPM method, while the CP method is for customers who use other platforms (e.g., Microsoft Windows) that do not support the RPM install option.

The hash values listed under each item above are being used to check the integrity of the packages and documents before installation. Please note that the patch in jboss-eap-6.2.2.zip needs to be applied to the jboss-eap-6.2.0.zip or jboss-eap-6.2.0-installer.jar deliverables.

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:

- The TOE must ensure that only identified and authorized users gain access to the TOE and its resources.
- The TSF must control access to resources based on identity of users. The TSF must allow authorized users to specify which resources may be accessed by which users.
- The TSF must control access to administrative resources as well as administrative operations based on the role a user is assigned to. The TSF must allow authorized users to specify which resources may be accessed by which users.
- The TSF must record security relevant actions of users of the TOE. The information recorded with security relevant events must be in sufficient detail to help an administrator of the TOE detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
- The TSF must ensure the consistency of user data as well as TSF data while it is being processed. Consistency needs to be ensured when data is processed that may be located in multiple places.

4. Assumptions and Clarification of Scope

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

- Those responsible for the administration of the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
- Those responsible for the TOE must ensure that the operating system and the Java virtual machine are installed and configured in accordance with the guidance of the TOE and that these mechanisms operate as specified. This also covers that only the Java virtual machines enumerated in this ST are used as underlying platform to ensure that proper date and time information is available to the audit facility.

- Those responsible for the TOE must establish and implement procedures to ensure that the software components that comprise the TOE are distributed, installed, configured and administered in a secure manner.
- Those responsible for the TOE must ensure that those parts of the TOE critical to security policy as well as the underlying hardware and software are protected from physical attack which might compromise IT security objectives.
- Those responsible for the TOE must ensure that procedures and/or mechanisms are provided to assure that, after system failure or other discontinuity, recovery without a protection (i.e. security) compromise is obtained.
- Those responsible for the TOE shall ensure that the developers of the applications executed by the TOE are trustworthy and implement the applications in accordance with the guidance provided with the TOE.

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

5. Architectural Information

JBoss Enterprise Application Platform 6, Version 6.2.2 implements a system for innovative and scalable Java applications. It includes open source technologies for deploying, and hosting enterprise Java applications and services.

JBoss Enterprise Application Platform balances innovation with enterprise class stability by integrating the most popular clustered Java EE application server with next generation application frameworks. Built on open standards, JBoss Enterprise Application Platform integrates various containers implementing the Java EE functionality, and other containers providing mechanisms to applications which go beyond the Java EE standard into a complete, simple enterprise solution for Java applications.

The Java EE specification considers the four layers listed in table 3, also called tiers. Applications utilizing the Java EE specification may implement any combination of these tiers. In addition to listing the tiers, the following table specifies which tiers can be implemented and executed using the framework of JBoss.

Java EE Tier	JBoss coverage
Client tier The client tier is the layer of the application executed on the client system in order to display the information provided by the application server. The client tier can be implemented by: ● An applet executed by the client's browser ● A stand-alone Java application executed by the client's Java Virtual Machine ● The HornetQ client	The applet may be stored on the JBoss server in order for the client to automatically download it when accessing a web page served by JBoss. However, neither the applet nor the application is executed by the JBoss application server, but they are executed by the Java Virtual Machine of the client system accessing the JBoss information remotely. Therefore, the client tier is considered to be not covered by JBoss.
Web tier The web tier is the presentation layer of the application server. It gathers the business information from the lower EJB tier and converts it to be presented as web pages. The web tier therefore does not implement any business logic as it can be considered an information converter from the application-internal data representation to a user-viewable and user-interpretable presentation. Considering a web-shopping application, the web tier implements the presenting layer with functionality such as the web pages showing the sold products or the display of the contents of the user's shopping cart.	The web tier can be implemented using Java servlets executing within the JBoss framework. The web tier is implemented by the customer-developed application.
Enterprise Java Beans (EJB) tier The EJB tier implements the business logic of the entire application. Business logic is considered to be the functionality implementing the information flow consistent with the purpose of the application. Considering a web-shopping application, the EJB tier implements business logic, such as the management and maintenance of the sold products, the shopping cart for each user.	The EJB tier can be implemented using various types of EJBs executing within the JBoss framework. The EJB tier is implemented by the customer-developed application.
Enterprise Information System's tier	The enterprise information system's tier is

Java EE Tier	JBoss coverage
The enterprise information system's tier provides the logic to allow the EJB tier to access external data stores. This tier therefore covers database access mechanisms, such as a JDBC driver.	provided by the TOE allowing the application's EJBs to access relational databases listed for JDBC. The enterprise information system's tier is implemented by the TOE.

Table 3: Java EE tier listing and JBoss coverage

Fundamentally in the JBoss architecture, the JBoss server subsystem manages the set of pluggable component services which are either implemented as POJOs or as MBeans. This allows the assembly of different configurations and provides the flexibility to tailor configurations to meet specific requirements.

The administrator does not have to run a large, monolithic server all the time; as components not needed (which can also reduce the server startup time considerably), can be removed. Also, additional services can be integrated into JBoss by writing new MBeans. In addition, POJOs configured as services can be created for either extending the JBoss functionality or implementing business logic.

Figure 1 shows the interoperation of the different components of JBoss. JBoss consists of a modular framework where the administrator can selectively enable components. JBoss EAP offers compliance with the Java EE 6 specification and offers services beyond Java EE. The following description applies to the figure:

- The hardware together with the operating system executes the Java virtual machine which in turn executes the JBoss Modules framework. This framework provides the foundation on which all JBoss containers perform their tasks.
- Each container implements either a service as specified in Java EE 6 or a service providing additional functionality beyond Java EE 6.
- Applications execute as part of containers (such as the JAX-RS Web Services container or the EJB container) and may utilize services from other containers.

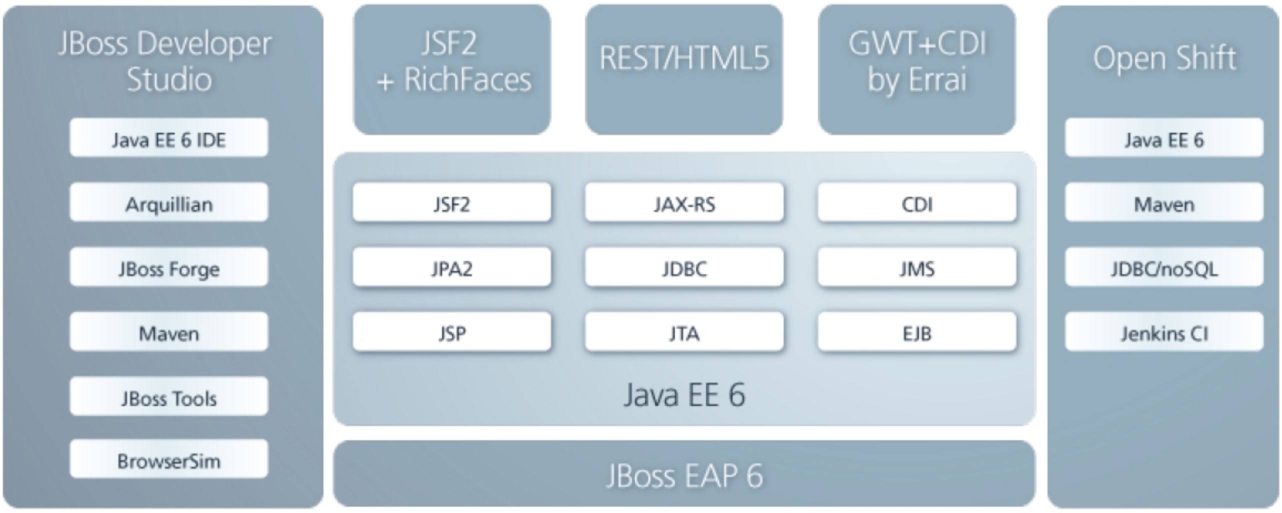

Figure 1: JBoss components

The TOE allows the interaction with users through the following services:

- HTTP web network protocol
- Webservices
- Enterprise Java Beans (EJB)
- HornetQ Java Messaging Service (JMS)
- Java Naming and Directory Interface (JNDI)

Applications utilize the services provided by the different containers by accessing the API exported by each container. These applications are loaded and executed by either the JSP/Servlet container, EJB container or other containers. The technical separation of the untrusted applications and the TOE is achieved using the Java Security Manager with an appropriate policy configuration.

6. Documentation

The evaluated documentation as outlined in table 2 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

Testing approach

The test mapping document provided by the developer lists the tree of test suites which comprises of test cases which in turn comprise of the test units. This mapping document also provides the ability to trace the individual test unit back to the interfaces that the test unit covers.

The tests are written in Java and are completely automated and available online at the same URL as the JBoss TOE source code. The tests include applications which are loaded onto the TOE as well as user programs which try to access the applications by interfacing with the TOE.

The test cases contain information about the desired/expected behaviors and validates whether the TOE acts according to the expected behavior(s). If the TOE acts as expected, a pass result is returned to the test framework, otherwise, a fail is returned. The test framework records and collects the test results and present them in human-readable HTML files.

Test configuration

The testing of the TOE was performed several times with different configuration constraints. The following constraints were considered by the developer:

- The testing was executed with the Java Security Manager and its well-defined policy enabled.
- Testing was performed on all JDKs specified in the ST.

- All user account data stores allowed in the ST were covered by the tests.
- The different databases listed in the ST were used as a database backend.
- User data store of LDAP, database and properties files are tested.

Testing was performed on the TOE version specified in [6] and [8]. Additionally, the test environments and test platforms were configured to be compliant with requirements of the evaluated configuration as dictated in [6] and [8]. Therefore, the testing configurations meet the configuration requirements for the evaluated configuration.

Test coverage

The test case mapping identifies the interfaces to which the test cases map. The following types of TSFI are covered by the tests:

- Network protocols enforcing access control and identification and authentication configurations.
- Source code annotations for configuring access control functionality.
- Configuration files and deployment descriptors for the configuration of the identification and authentication and access control functionality. In addition, transaction support is tested using deployment descriptors.
- The command line interface is indirectly covered by starting the TOE in two different modes of operation, which can only be done using appropriate command line switches.

Test depth

The test depth, i.e., the coverage of all subsystems implementing SFR-enforcing functionality, is also provided by the same tests described above for the test coverage. The test mapping document maps test cases to applicable subsystems. The test depth analysis shows that the test cases not only cover the subsystems they invoke directly but also the subsystems that can only be triggered indirectly.

Testing results

The test results provided by the developer were generated on the JDK platforms and configurations outlined above. As described in the testing approach, the test results for all these automated tests are recorded and collected by the framework and written to HTML files.

All test results from all tested configurations show that the expected test results are consistent with the actual results.

7.2. Evaluator Testing

Testing approach

In addition to repeating all developer tests on the above-mentioned system configuration/scenario, the evaluator devised tests for a subset of the TOE functionality.

The tests were chosen by the evaluator based on the following reasons:

- Audit configuration in the evaluated configuration adds an additional audit trail file.
- A large number of different interfaces are invoked by the developer testing.
- Different access control functions are covered by the developer testing.

- As the developer test cases already cover the central TOE functions with a large number of tests, the evaluator focused on minor security functionality that was covered only lightly by the developer testing.
- The HTTP HEAD access type was not covered in the developer testing for verifying the access control enforcement for HTTP connections.

Test configuration

As part of the independent testing, the evaluator installed the TOE using the CC Guide [8] and the product installation documentation [10]. The test cases are prepared as described in the developer test plan. The evaluator concluded that the evaluator's test configuration was consistent with the ST [6] and the CC Guide [8], i.e. it is covering the following issues:

- RHEL 5.9 x86_64
- OpenJDK JRE 1.6
- Local file-based user definition

Test depth

The evaluator created his own test cases expanding the functional aspects of auditing and HTTP access control. Through examination of the developer test cases, the evaluator gained sufficient confidence in the developer test effort as well as coverage. The developer tests were shown to demonstrate a very wide coverage of the TSF, therefore, the evaluator decided to devise only a small number of additional test cases.

Testing results

The evaluator testing effort consists of two parts: repetition of the developer tests and execution of the tests created by the evaluator.

The test system was set up as stated above. When rerunning the developer tests using one specific test scenario configuration executed by the developer, the evaluator used the developer test plan to set up and initiate these tests. All tests were executed successfully and test results were recorded in a test result file.

The independent tests of the evaluator covered the following functional areas:

- Auditing: different tests were executed covering different functional areas of the TOE to verify that appropriate audit records are created and maintained by the TOE for the access requests.
- HTTP access control: the evaluator tested the enforcement of the HTTP access control policy on the HEAD HTTP request type.

All tests passed successfully.

7.3. Evaluator Penetration Testing

Testing approach

The evaluator took the following approach to derive penetration tests for the TOE: First the evaluator checked common sources for vulnerabilities of the JBoss server in general and the TOE in particular. The evaluator determined:

- Whether the reported vulnerability would affect the evaluated configuration of the TOE in its intended environment. If yes, the evaluator performed a vulnerability analysis.

- Whether the reported vulnerability has already been fixed in the evaluated configuration of the TOE. If the reported vulnerability does not have a fix, the evaluator analyzed the potential impact and exploitability.

Beside those vulnerabilities reported in common sources, the evaluator checked the evaluation reports for potential vulnerabilities mentioned within those reports. For those vulnerabilities, the evaluator devised a way to check for the existence or absence of the hypothetical vulnerability, while taking into account that the TOE is an Open Source product and so the evaluator had full access to the source code.

Based on the vulnerability analysis, the evaluator conducted testing in the following areas:

- Verification of whether the fix for a security issue is effective.
- Verification of the effectiveness of access control of a typically unused and rarely known HTTP request type.
- Verification that shared components maintaining sensitive information do not leak them.

Test configuration

The evaluator performed his penetration tests on a TOE that was installed and configured according to the CC guidance [8].

Test depth

Although the evaluator decided to only generate a small number of penetration tests, for some of the identified potential vulnerabilities, the evaluator performed a very extensive analysis exceeding the requirements of EAL4 claimed by the TOE. The reasons are as follows:

- The TOE as an open source product is already subject to the scrutiny of obvious vulnerabilities by the Open Source community, thus, simple and high-level penetration testing was deemed insignificant by the evaluator.
- The TOE as an open source product is delivered with full source code, thus, allowing the evaluator the means to perform an extensive analysis which is usually considered inconceivable for products evaluated at an EAL4 assurance level. In general, the evaluator considered source code review as a more effective method for vulnerability analysis than testing. Due to the nature of vulnerabilities, a perceived vulnerability is usually obscure in reality and therefore only exploitable when meeting certain constraints. Testing may not cover all constraints (as certain constraints are not fully defined or known to testers), thus, a test yielding no vulnerability does not necessarily demonstrate that no vulnerability is present.

Test results

The penetration testing addressed the following security functionalities:

- Non-bypassibility of TOE security functions

No vulnerability was detected.

8. Evaluated Configuration

This certificate covers the following configurations of the TOE: The TOE is JBoss Enterprise Application Platform 6, Version 6.2.2. The items listed in table 2 of this report represent the TOE.

The Security Target [6] states the following requirements for the operational environment of the TOE:

Operating Systems:

- RedHat Enterprise Linux 5 (x86 and x86_64)
- RedHat Enterprise Linux 6 (x86 and x86_64)
- Solaris 10 (x86 and x86_64, Sparc)
- Solaris 11 (x86 and x86_64, Sparc)
- Microsoft Windows Server 2008 (x86 and x86_64)
- Microsoft Windows Server 2008 R2 (x86_64)
- Microsoft Windows Server 2012 (x86_64)

Additionally, the Operational Environment for the TOE allows the use of one of the following JDKs:

- OpenJDK 1.6.x
- OpenJDK 1.7.x
- Oracle JDK 1.6.x
- Oracle JDK 1.7.x
- IBM JDK 1.6.x
- IBM JDK 1.7.x

For providing the cryptographic services supporting the SSL/TLS protocol on which the certificate-based authentication relies on, the TOE uses the standard cryptographic service providers shipped with the above mentioned Java Runtime Environments.

Native code, such as OpenSSL or libAIO for Red Hat Enterprise Linux is not used in the evaluated configuration.

As the TOE functionality only relies on the correct operation of the Java virtual machine, the TOE can be executed on any operating system that is supported by the respective Java virtual machine. This also means that any hardware supported by the aforementioned operating systems can be used to execute the TOE.

The following relational databases are allowed to be used with the TOE (the listed databases are part of the operational environment and therefore not covered with security claims in the Security Target [6]):

- IBM DB2 9.7
- IBM DB2 10.1
- Oracle 11g R1
- Oracle 11g R1 RAC
- Oracle 11g R2
- Oracle 11g R2 RAC
- Oracle 12c
- MySQL 5.5

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- PostgreSQL 9.2
- Enterprise DB 9.2
- Sybase ASE 15.7

The internal database (H2 DB) is not supported in the evaluated configuration.

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.

The Evaluation Methodology CEM [2] was used.

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.3 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0687-2011, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on major differences between the previously certified TOE and the new version:

- The core JBoss EAP architecture based on the JBoss Microkernel has been replaced by an architecture supported by JBoss Modules.
- Administrative actions to be performed on either the system configuration or the system state are subject to role-based access control. A set of default management roles is delivered with the initial installation of the TOE:
- A number of new mechanisms specified in the Java EE community process are implemented.
- The primary security subsystem of JBoss, JBossSX, is replaces by PicketBox.
- The JBoss JMS implementation is replaced with HornetQ.
- JBoss Cache is replaces by Inifispan which is a re-implementation of JBoss Cache.
- The high-availability support of JNDI is removed.
- The JBoss system configuration file is either domain.xml or standalone.xml depending on the startup mode of JBoss or a configuration file specified via a command line option.
- The list of underlying operation system, JDK and accessible databases is updated to match the current technology.

The evaluation has confirmed:

● for the Functionality:	Product specific Security Target Common Criteria Part 2 extended
● for the Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

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 cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

10. Obligations and Notes for the Usage of the TOE

The 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, Threats and OSPs 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 of the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

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
cPP	Collaborative Protection Profile

EAL	Evaluation Assurance Level
EAP	Enterprise Application Platform
EJB	Enterprise Java Beans
ETR	Evaluation Technical Report
HTTP	Hypertext Transfer Protocol
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
JAAS	Java Authentication and Authorization Service
Java EE	Java Enterprise Edition
JAX-RS	Java API for RESTful Web Services
JBOSS SX	JBoss Security Framework
JDBC	Java Database Connectivity
JDK	Java Development Kit
JMS	Java Messaging Service
JMX	Java Management Extension
JNDI	Java Naming and Directory Interface
JTA	Java Transaction API
MBeans	Managed Bean
POJO	Plain Old Java Object
PP	Protection Profile
RBAC	Role-Based Access Control
RHN	Red Hat Network
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

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

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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

Informal - Expressed in natural language.

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

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

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 - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[3] BSI certification: Technical information on the IT security certification of products, protection profiles and sites (BSI 7138) and Requirements regarding the Evaluation Facility for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC (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-CC-0909-2015, Version 1.1, 2014-09-26, RedHat JBoss Enterprise Application Platform 6 Version 6.2.2 Security Target, Red Hat and atsec information security

[7] Evaluation Technical Report, Version 5, 2015-01-30, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[8] Red Hat JBoss Enterprise Application Platform Common Criteria Certification 6.2.2 Common Criteria Configuration Guide, Version 6.2.2, 2014-06-24

[9] JBoss API JavaDoc, Version JBoss EAP 6.2.2, 2014-03-31

[10] JBoss Enterprise Application Platform Common Criteria Certification 6.2 Installation Guide, Version 2.0-23, 2014-02-14

[11] JBoss Enterprise Application Platform 6.2 Administration and Configuration Guide, Version 6.2, 2014-03-10

[12] JBoss Enterprise Application Platform 6.2 Development Guide,Version 6.2, 2014

[13] HornetQ User Manual, Version 2.3, 2012

[14] Red Hat JBoss Enterprise Application Platform Common Criteria Certification 6.2.2 Security Guide, Version 6.2.2-14, 2014-05-21

[15] SVN CI list of User guidance and CC evidence, Date received 2014-06-25

[16] Red Hat JBoss Enterprise Application Platform Common Criteria Certification 6.2.2 Common Criteria Configuration Guide, Version 6.2.2, Date 2014-06-24

[17] CI for RHEL 5 architecture, Date received 2014-06-24

[18] CI for RHEL 6 architecture, Date received 2014-06-24

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

C. Excerpts from the Criteria

CC Part 1:

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-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

Assurance Class	Assurance Components
	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: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	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.

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

“Objectives

EAL 1 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.

EAL 1 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.

EAL 1 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 EAL 1 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 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 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.

EAL 2 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 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 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 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 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. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 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 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 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 EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 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 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 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.

EAL 6 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 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
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”

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."

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.