Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0450-2008

for

IBM WebSphere Message Broker Version 6.0.0.3

from

IBM United Kingdom Limited

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-0450-2008

message queueing software

IBM WebSphere Message Broker
Version 6.0.0.3

from	IBM United Kingdom Limited
Functionality:	Common Criteria Part 2 extended by FAU_GEN_(EXP).1
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2

Common Criteria
Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed / approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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, 13 June 2008

For the Federal Office for Information Security

IT
Security
Certified

SOGIS - MRA

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, Version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria 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 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria 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 IBM WebSphere Message Broker Version 6.0.0.3 has undergone the certification procedure at BSI.

The evaluation of the product IBM WebSphere Message Broker Version 6.0.0.3 was conducted by atsec information security GmbH. The evaluation was completed on 20th May 2008. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: IBM United Kingdom Limited

The product was developed by: IBM United Kingdom Limited

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 and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular 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 IBM WebSphere Message Broker Version 6.0.0.3 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://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] IBM United Kingdom Limited
Hursley Park
Winchester
Hants. SO21 2JN

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 IBM WebSphere Message Broker, Version 6.0.0.3. WebSphere Message Broker (WMB) enables information, packaged as messages, to flow between different business applications, ranging from large legacy systems to unmanned devices such as sensors on pipelines. WMB provides the routing and data transformations necessary for the applications to communicate with one another. Communications between an application and WMB are via the WebSphere Message Queue (MQ) transport.

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

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C or [3], part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL4 augmented by ALC_FLR.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.2. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.3.

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

TOE Security Function	Addressed issue
Security audit	WMB performs security auditing for all Toolkit Policy accesses made to the TOE. Audit records are generated when audit events occur. The audit records include the responsible user, date, time, and other details. The audit data is recorded into the operating system for protection.
Communication	WMB provides message flow control of messages flowing through the broker. The nodes control the routing of messages (by the way they're connected within a message flow and by routing decisions made within certain nodes) and the transformation of messages.
Security Management	WMB provides security management functionality for the management of the access control policies. Management is performed from the command line.
Protection of the TSF	WMB protects itself and ensures that its policies are enforced in a number of ways. First, WMB interacts with users through well-defined interfaces designed to ensure that the WMB security policies are always enforced. Next, WMB encrypts all communications between physically separate parts of the TOE to ensure that no data is disclosed or modified.
User Data Protection	WMB protects user data by providing access control lists (ACLs) which mediate access between users and WMB objects.

Table 1: TOE Security Functions

For more details please refer to the Security Target [6], chapter 6.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 2. Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the following configurations of the TOE: The TOE architecture consists of three subsystem functional components: Message Brokers Toolkit, Broker and Configuration Manager. Additionally, the IT environment consists of the Applications (Clients) which use the TOE, databases used by the TOE, a repository used by the TOE, the MQ transport, the Java Runtime Environment (JRE), and the underlying operating systems. The Security Target defines various operating systems allowed to be used for the broker and Windows XP for the configuration manager as well as the toolkit. For details refer to chapter 8 of [6].

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:

IBM WebSphere Message Broker Version 6.0.0.3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	IBM WebSphere Message Broker	6.0.0.3	CD / electronic download
2	SW	IBM WebSphere Message Broker, (Version 6.0.0.0 with an additional CD or download of FixPack 3)	6.0.0.0	CD / electronic download
3	DOC	[WMBADM] Configuration, Administration, and Security	6.0	CD / electronic download
4	DOC	[WMBCCGUIDE] Common Criteria ReadMe, 27.09.2007	1.7	CD / electronic download
5	DOC	[WMBINSTALL] Installation Guide, 06.12.2007	6.0	CD / electronic download

Table 2: Deliverables of the TOE

No hardware is delivered with the product. For further guidance documents see chapter 6.

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:

WMB provides protection of the communication via message flow control of messages flowing through the broker. Security auditing for all Toolkit Policy accesses made to the TOE, also as security management functionality for the management of the access control policies are provided. WMB protects itself and ensures that its policies are enforced in a number of ways and it protects user data by providing access control lists.

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, such as A.NO_EVIL, A.INSTALL_REQ, A.NETWORK, A.PHYSICAL and A.PLATFORM. Details can be found in the Security Target [6] chapter 3.2.

Further, objectives are defined which need to be fulfilled by the TOE-environment. These are OE.AUDIT_STORAGE, OE.USER_AUTHENTICATION, OE.SECURE_TRANS, OE.USER_IDENTIFICATION, OE.TIME, OE.TOE_PROTECTION and OE.PLATFORM (see ST [6], chapter 4.2). Referring to the non-IT environment, the following objectives are defined in the Security Target [6], chapter 4.3 to fulfil the above mentioned assumptions: OE.ADMIN_GUIDANCE, OE.CONFIG, OE.INSTALL, OE.PHYSICAL and OE.SELF_PROTECTION.

5 Architectural Information

5.1 General overview of WMB

The Target of Evaluation (TOE) is IBM WebSphere Message Broker, Version 6.0.0.3.

WebSphere Message Broker (WMB) enables information, packaged as messages, to flow between different business applications, ranging from large legacy systems to unmanned devices such as sensors on pipelines. WMB provides the routing and data transformations necessary for the applications to communicate with one another. Communications between an application and WMB are via the WebSphere Message Queue (MQ) transport1.

There are two ways in which WMB can act on messages:

Message routing from sender to recipient based on the content of the message where WMB can be configured for message routing via message flows that can be designed. A message flow describes the operations to be performed on the incoming message, and the sequence in which they are carried out. Each message flow consists of: A series of steps used to process a message, as defined in message flow nodes, and connections between the nodes that define the routes through the processing. Connections are made using message flow node connections. WMB provides built-in nodes and samples for numerous common functions. Additional functions can be built using a simple Graphical User Interface (GUI) to create user-defined nodes.

Message transformation before being delivered from one format to another by modifying, combining, adding or removing data fields. Transformations can be made by various nodes in a message flow but before a message flow node can operate on an incoming message, it must understand the structure of that message such as: some messages contain a definition of their own structure and format known as self-defining messages that can be handled without the need for additional information about the structure and format; and, other messages do not contain information about their structure and format. To process them later, a message definition of their structure must be created and made available. The message definitions defined are created within a message set which contains one or more message definitions. Like message flows, message definitions are built using GUI actions that contain two types of information: the logical structure - the abstract arrangement and characteristics of the data, represented as a tree structure; and, one or more physical formats - the way the data is represented and delimited in the physical bitstream.

5.2 Major structural components within WMB

- Broker and broker nodes: The broker is a set of different Windows services or Unix daemons. The broker covers the message flow mechanism which consist of nodes which are connected to each other by using the output terminal of one node and linking it to the input terminal of another node. Based on the management of these connections between terminals, no terminal is left unconnected when a node gets destroyed. During the destruction, the node sends notifications to the neighbour nodes informing them about the change in connections. The start point and end point of message flows are the MQInput and MQOutput nodes which receive/send messages from/to message queues (although the MQGet node also can retrieve messages from message queues, this node is to be used for retrieving messages from queues within a message flow, but not as a starting point for a message flow).
- Configuration manager: The configuration manager is a subsystem which manages one or more brokers and establishes the connection to users configuring the message flows. It receives messages from different sources and handles the message flows as well as the message definitions accordingly. When deploying a message flow, the configuration manager contacts the appropriate broker and submits the message flow definition to it.
- Command line applications: The command line applications are used for configuring the broker and the configuration manager.
- Message broker toolkit: The toolkit is an extensive GUI allowing the administrator and the developer of message flows to effectively generate such message flows and configure the configuration manager as well as the brokers.

6 Documentation

The evaluated documentation as outlined in table 2 of this report 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.

[CMPAPI]	JavaDoc of Configuration Manager Proxy API
[WMBADM]	Configuration, Administration, and Security, Version 6.0, 2007-12-06
[WMBCCGUIDE]	Common Criteria ReadMe, Version 1.7 , 2007-09-24
[WMBCMP]	CMP Programming, Version 6.0, 2007-12-06
[WMBDIAG]	Diagnostic Messages, Version 6.0 FP4
[WMBESQL]	ESQL, Version 6.0, 2007-12-06
[WMBICUNIX]	WebSphere Message Broker Information Center for Linux, Version 6.0, 2007-12-06
[WMBWIN]	WebSphere Message Broker Information Center for Windows, Version 6.0, 2007-12-06
[WMBINSTALL]	Installation Guide, Version 6.0, 2007-12-06
[WMBINTRO]	Introduction, Version 6.0, 2007-12-06
[WMBMF]	Message Flows,Version 6.0, 2007-12-06
[WMBMM]	Message Models, Version 6.0, 2007-12-06
[WMBTS]	Troubleshooting, Version 6.0, 2007-12-0

7 IT Product Testing

The Security Target defines various operating systems allowed to be used for the broker and Windows XP for the configuration manager as well as the toolkit.

7.1 Report on the developer testing effort

Test configuration

The test results for the node tests provided by the developer were generated on the following operating systems:

- RHEL4 AS
- SunOS 5.9
- Windwos 2003 Server
- AIX 5.3 ML02
- RHEL4 U4 (z/Series)
- RHEL4 AS (POWER)
- HP-UX 11.11
- Windows XP

The test results for the configuration manager manual tests are provided for the testing conducted on a Windows XP system.

Testing approach

The FSP mapping document provided by the developer lists test cases for the different TSF/TSFI the test cases are associated with. The test plan for the different tests is focused on the security functions of the TOE and ignores other aspects typically found in developer test plans. The test cases are mapped to the corresponding Functional Specification and HLD.

Testing is conducted with two different test approaches:

- Manual test cases requiring the use of command line tools and the Websphere Message Broker toolkit verify the functionality of the configuration manager.
- Automated tests perform the testing of the different nodes allowed to be used in the evaluated configuration. The test cases are independent and configure the necessary message flow with the tested node directly by interfacing with the message queues used for communication between the configuration manager and the broker.

Test results

The test results provided by the developer were generated on the operating systems listed above for the node tests. The test results of all the automated tests are written to files.

The test results of the manual tests have been recorded by the developer and those results are presented as part of the test documentation of these manual tests.

All test results from all tested platforms show that the expected test results are identical to the actual test results.

Test coverage

The functional specification has identified different TSFI:

- command line applications (including the maintenance of configuration files)
- CMP API for the configuration manager
- all different nodes

A mapping provided by the sponsor shows that the tests cover all individual TSFI identified for the TOE. An extension to this mapping developed by the evaluators as documented in the test case coverage analysis document show that also significant details of the TSFI have been tested with the developer's testing.

Test depth

In addition to the mapping to the functional specification, the sponsor provided a mapping of test cases to subsystems of the high level design. This mapping shows that all subsystems are covered by test cases. Using the high-level design, the coverage of internal interfaces was evident. To show evidence that the only one internal interface between the configuration manager and the broker has been called, the automated test cases testing the nodes are analysed. These test cases configure the message flow by directly using the internal interface to the broker.

7.2 Report on the evaluator testing effort

TOE test configuration

The evaluator independently installed the test systems considering the instructions found in the CC guide, WMB installation and administration guidance, and the test documentation for the manual test cases. The CC guide instructions achieve the evaluated configuration which is consistent with the ST. Hence, the evaluator concludes that the evaluator's configuration is consistent with the ST.

The evaluator used the following operating systems for testing:

- Windows XP: The Windows XP Professional system was used to execute the toolkit, the configuration manager and several instances of the broker.

The communication was established using the provided WebSphere message queue system.

- RHEL4 AS: The RHEL4 AS on IA32 hosted several instances of the broker connected to the configuration manager via WebSphere message queues over TCP/IP.

Subset size chosen

The evaluator re-performed test cases out of the set of manual test cases. The evaluator considered that the chosen sample covers the different areas of testing listed the manual test documentation, covering the ACL mechanism as well as the secure management functionality.

Evaluator tests performed

The evaluator devised tests for a subset of the TOE. The tests are listed in the evaluator's test plan.

The evaluator has chosen these tests for the following reasons:

- The test cases examine some edge-conditions where the evaluator considers more testing is necessary than performed by the developer (ACL mechanism, message flows).
- As the sponsor-supplied test cases already cover the security functionality of the TOE in a broad sense the evaluator has devised only a small set of test cases.

The evaluator created several test cases for testing a few functional aspects where the sponsor test cases were not considered by the evaluator to be broad enough. During the evaluator coverage analysis of the test cases provided by the sponsor, the evaluator gained confidence in the sponsor testing effort and the depth of test coverage in the sponsor supplied test cases.

Summary of evaluator test results

The evaluator testing effort consists of two parts. The first one is the observation of the developer's test approach and execution of test cases and the second is the execution of the tests created by the evaluator.

The testing was conducted at the evaluation lab in Cologne, Germany.

The TOE was installed on all machines by the evaluator according to the instructions in the CC guide and the manual test documentation.

When executing the developer tests, the evaluator was immediately able to observe whether a test case succeeded or failed. The test documentation contains sufficient instructions to interpret the observed behaviour and to determine whether the TOE behaves as intended.

In addition to running the tests that were provided by the sponsor according to the test plan from the sponsor, the evaluator decided to run some additional test cases:

- Audit tests: verification of audit generation.
- different ACL tests to verify edge conditions
- creation of different message flows to verify edge conditions

All tests passed successfully.

Summary of the evaluator penetration testing

The evaluator has devised a set of penetration tests based on the developer's vulnerability analysis and based on the evaluator's knowledge of the TOE gained by the other evaluation activities. All penetration tests have been designed to require only a low attack potential as defined in AVA_VLA.2. The evaluator conducted those tests and did not find any test that resulted in a penetration of the TOE with low attack potential. Also the vulnerability analysis did not identify any vulnerability that could be exploited with low attack potential. Therefore the evaluator has determined as a result of his activities that the TOE is resistant against attacks with low attack potential.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE is comprised of the WMB components created by IBM. The TOE architecture consists of three subsystem functional components, which are placed at key points within the Enterprise architecture: Message Brokers Toolkit, Broker, and Configuration Manager. Additionally, the IT environment consists of the Applications (Clients) which use the TOE, databases used by the TOE, a repository used by the TOE, the MQ transport, the Java Runtime Environment (JRE), and the underlying operating systems. Figure 1 below shows these components (excluding the OS), their location, and interaction in the architecture.

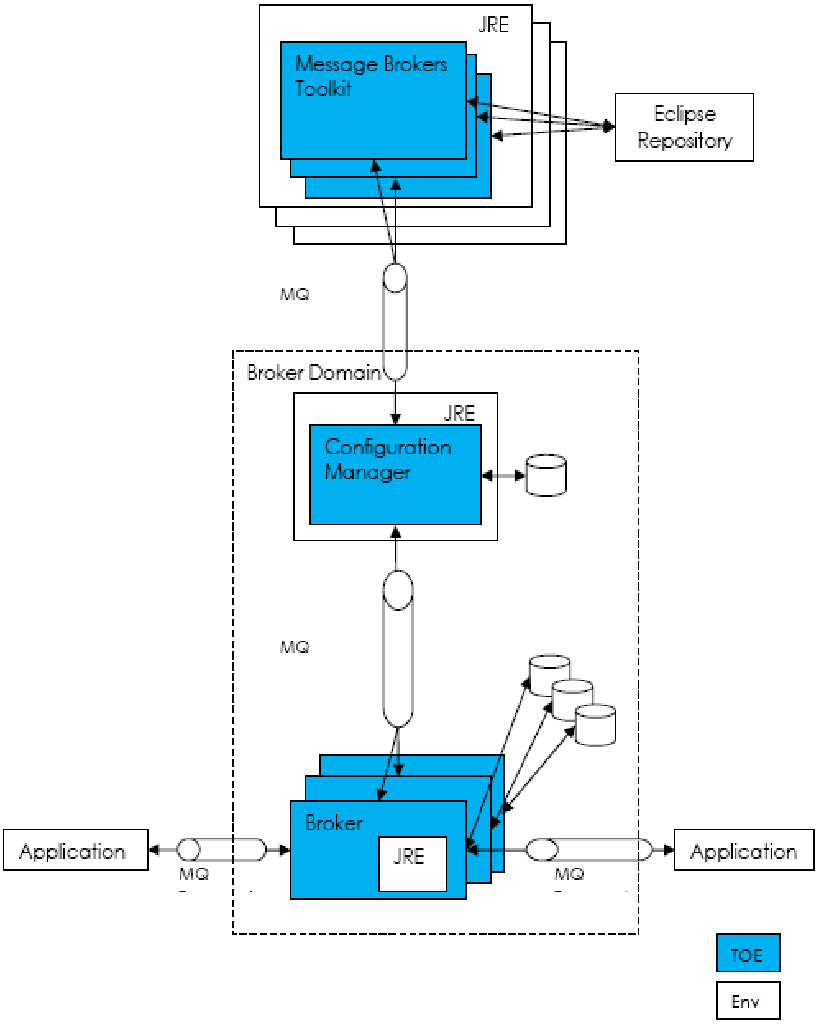

Figure 1: TOE and environment

Brokers are logically divided into Broker Domains. A collection of Brokers, that share a common Configuration Manager form a broker domain. The Broker and Configuration Manager components run within a specific Broker Domain environment and work together to enforce the overall TOE security policies. The Message Brokers Toolkit component utilizes the business integration repository.

Physical Boundaries

Each of the TOE components is a software application designed to execute within an operating system context provided by the environment. The Message Brokers Toolkit is an Eclipse application – which is based on Rational Application Developer version 6. The Configuration Manager is a Java application with a C++ wrapper. The Broker is a C/C++ application that uses JRE to perform some of its functions.

The evaluated configuration is supported on the following operating systems:

- AIX 5.3 – RS/6000 (POWER)
- HP-UX 11i – PA-RISC
- Red Hat Enterprise Linux (RHEL) AS4 for IA32
- RHEL AS4 for POWER

- RHEL AS4 for zSeries
- Solaris 9 - SPARC
- Windows XP Pro
- Windows Server 2003 Standard Edition, Enterprise Edition, and R2

The evaluated configuration requires a database that uses the ODBC protocol. The supported databases are:

- IBM DB2 v9.1 except on HP-UX
- IBM DB2 v8.2 on HP-UX only

The evaluated configuration supports WebSphere MQ 6.0.2.0. MQ contains and uses IBM's Global Security Kit (GSKit) library for SSL v3 and TLS v1.0.

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.

It was supplemented by the methodology for "ALC_FLR – Flaw remediation", Version 2.3, August 2005.

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

- All components of the class ASE
- All components of the EAL4 augmented package as defined in the CC (see also part C of this report)
- The components ALC_FLR.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the functionality: Common Criteria Part 2 extended by FAU_GEN_(EXP).1
- for the assurance: Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2
- No Strength of Function (SOF) is claimed.

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 documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

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

ACL	Access Control List
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JRE	Java Runtime Environment
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
WMB	WebSphere Message Broker

12.2 Glossary

Assets - Information or resources to be protected by the countermeasures of a TOE.

Assignment - The specification of an identified parameter in a component.

Assurance - Grounds for confidence that an entity meets its security objectives.

Attack potential - The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Authentication data - Information used to verify the claimed identity of a user.

Authorised user - A user who may, in accordance with the TSP, perform an operation.

Class - A grouping of families that share a common focus.

Component - The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Connectivity - The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.

Dependency - A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other

requirements to be able to meet their objectives.

Element - An indivisible security requirement.

Evaluation - Assessment of a PP, an ST or a TOE, against defined criteria.

Evaluation Assurance Level (EAL) - A package consisting of assurance components from Part 3 that represents a point on the CC predefined assurance scale.

Evaluation authority - A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.

Evaluation scheme - The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.

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.

External IT entity - Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Family - A grouping of components that share security objectives but may differ in emphasis or rigour.

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

Human user - Any person who interacts with the TOE.

Identity - A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

Informal - Expressed in natural language.

Internal communication channel - A communication channel between separated parts of TOE.

Internal TOE transfer - Communicating data between separated parts of the TOE.

Inter-TSF transfers - Communicating data between the TOE and the security functions of other trusted IT products.

Iteration - The use of a component more than once with varying operations.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Organisational security policies - One or more security rules, procedures, practices, or guidelines imposed by an organisation upon its operations.

Package - A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

Product - A package of IT software, firmware and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Reference monitor - The concept of an abstract machine that enforces TOE access control policies.

Reference validation mechanism - An implementation of the reference monitor concept that possesses the following properties: it is tamper-proof, always invoked, and simple enough to be subjected to thorough analysis and testing.

Refinement - The addition of details to a component.

Role - A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret - Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.

Security attribute - Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

System - A specific IT installation, with a particular purpose and operational environment.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

Transfers outside TSF control - Communicating data to entities not under control of the TSF.

Trusted channel - A means by which a TSF and a remote trusted IT product can communicate with necessary confidence to support the TSP.

Trusted path - A means by which a user and a TSF can communicate with necessary confidence to support the TSP.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

User - Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

User data - Data created by and for the user, that does not affect the operation of the TSF.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

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

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

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target BSI-DSZ-0450-2008, Version 2.1.2, 22.08.07, IBM WebSphere Message Broker, IBM Procurement Sourcing Buyer - General Procurement

[7] Evaluation Technical Report, Version 2, 20.05.08, WebSphere Message Broker 6.0.0.3, atsec information security GmbH (confidential document)

[8] [CILISTCC] Final Configuration Items List (S000, confidential document)

[9] [CMPAPI] JavaDoc of Configuration Manager Proxy API

[10] [WMBADM] Configuration, Administration, and Security, Version 6.0, 2007-12-06

[11] [WMBCCGUIDE] Common Criteria ReadMe, Version 1.7, 2007-09-24

[12] [WMBCMP] CMP Programming, Version 6.0, 2007-12-06

[13] [WMBDIAG] Diagnostic Messages, Version 6.0 FP4

[14] [WMBESQL] ESQL, Version 6.0, 2007-12-06

[15] [WMBICUNIX] WebSphere Message Broker Information Center for Linux, Version 6.0, 2007-12-06

[16] [WMBWIN] WebSphere Message Broker Information Center for Windows, Version 6.0, 2007-12-06

[17] [WMBINSTALL] Installation Guide, Version 6.0, 2007-12-06

[18] [WMBINTRO] Introduction, Version 6.0, 2007-12-06

[19] [WMBMF] Message Flows,Version 6.0, 2007-12-06

[20] [WMBMM] Message Models, Version 6.0, 2007-12-06

[21] [WMBTS] Troubleshooting, Version 6.0, 2007-12-06

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

- **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.”

“Assurance Class	**Assurance Family**
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements ”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.”

“Assurance Class	**Assurance Family**
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“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 11.1)

“Table 6 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 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 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, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“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 practice. 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 11.5)

“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 practices.

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 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 11.8)

“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 11.9)

“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.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

"Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.