Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0556-2009

for

IBM Tivoli Identity Manager
Version 5.0

from

IBM Corporation

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-0556-2009

Identity Manager

IBM Tivoli Identity Manager
Version 5.0

from	IBM Corporation
PP Conformance:	None
Functionality:	Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 3 augmented by ALC_FLR.1

Common Criteria
Recognition
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, 08 June 2009
For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

Certification

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] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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.

European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for certificates based on ITSEC became initially effective in March 1998.

This agreement on the mutual recognition of IT security certificates was extended in April 1999 to include certificates based on the Common Criteria for the Evaluation Assurance Levels (EAL 1 – EAL 7). This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The German Federal Office for Information Security (BSI) recognises certificates

---

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

issued by the national certification bodies of France and United Kingdom, and from The Netherlands since January 2009 within the terms of this agreement.

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

International Recognition of CC - Certificates

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

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

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

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 Tivoli Identity Manager Version 5.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0237-2006. Specific results from the evaluation process BSI-DSZ-CC-0237-2006 were re-used.

The evaluation of the product IBM Tivoli Identity Manager Version 5.0 was conducted by atsec information security GmbH. The evaluation was completed on 26. May 2009. 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 Corporation

The product was developed by: IBM Corporation

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

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.

[6] Information Technology Security Evaluation Facility

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.

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.

Publication

The product IBM Tivoli Identity Manager Version 5.0 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 Software Group, Tivoli
1540 Scenic Ave
Costa Mesa,
CA 92626-1408, USA

This page is intentionally left blank.

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.

Executive Summary

The Target of Evaluation (TOE) is the IBM Tivoli Identity Manager Version 5.0. 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 3 augmented by ALC_FLR.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.2.

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

TOE Security Function	Addressed issue
Auditing of activities	The TOE is capable of auditing internal events (e.g. the modification of provisioning policies or the creation of new users) by generating audit records for all transactions that are stored in a database provided by the IT environment. The TOE also offers functionality to review these audit records.
Identification and authentication	The TOE identifies users (including administrators) by user name and authenticates them by password. ITIM users are persons with an account on the TOE; they can be organized by memberships to ITIM groups.
Authorization (access control)	The ITIM server performs authorization for user actions, commonly referred to as requests, based on Access Control Item (ACI). ACIs can be assigned to ITIM groups and ACI principals (e.g. administrators).
Provisioning	Provisioning policies define the services the persons belonging to an organizational role shall have access to. If a person belongs to an organizational role defined within the TOE, and a provisioning policy specifies the entitlement of this organizational role to a certain service, the person is entitled to have an account on this service.
Service Reconciliation and Identity Feeds	The TOE provides the capability of gathering account information from managed resources. Reconciliation retrieves and compares user information stored on a managed resource with the corresponding data stored in the ITIM database.

Table 1: TOE Security Functions

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

The claimed TOE’s Strength of Functions 'moderate' (SOF-moderate) for specific functions as indicated in the Security Target [6], chapter 1.4 is confirmed.

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 Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

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.

Identification of the TOE

The Target of Evaluation (TOE) is called:

IBM Tivoli Identity Manager Version 5.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	IBM Tivoli Identity Manager Version 5.0	5	Download or CD
2	DOC	Guidance documentation [9] - [18]		Download or CD

Table 2: Deliverables of the TOE

Security Policy

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

Provisioning access control and ITIM access control.

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: OE.AUDIT, OE.COM_PROT, OE.DB_PROT, OE.DIR_PROT, OE.ENFORCEMENT and OE.MANAGED. Details can be found in the Security Target [6] chapter 4.2.

Architectural Information

General overview

Identity management is a commonly used term for the central management of user identities that need to be available throughout a number of systems in a distributed operating environment. In large computer networks operated by organizations with many employees, an employee typically needs accounts on several operating systems and applications provided across the network infrastructure. As a result, the problem of managing the user accounts on each of those systems separately (e.g., an email system, a work flow application, a collaboration solution, shared resources, etc.) becomes very complex and costly. In addition, significant security risks arise from having each user maintain many different account credentials.

The IBM Tivoli Identity Manager (ITIM) provides a solution for managing the identity records that represent people in a business organization. ITIM is an identity management

solution that centralizes the process of provisioning resources, such as provisioning accounts on operating systems and applications to users. An ITIM identity represents the subset of profile data that uniquely represents a person in one or more repositories, and includes additional information related to the person. People, e.g. employees of an organization, obtain user accounts within ITIM which link the person's identity with their user profile and credentials.

ITIM uses the user account information and interacts with services (i.e. the computer systems) in a network infrastructure to provide user account services to these systems. To manage the user accounts ITIM relies on connectors that direct the management of accounts to so-called adapters: software components that sit either directly on the remote system, e.g. on the operating system, interacting with the user management mechanisms of the operating system, or on a central adapter server with network interfaces to the managed system. Provisioning is the procedure for interacting with the connectors and retrieving appropriate information for account creation for that identity to each of these services, or managed resources. ITIM uses policies, which represent sets of rules specifying within ITIM which identity shall have access to which of the services managed by ITIM.

In general, identities within ITIM are managed by membership of Organizational Roles and ITIM Groups:

- Organizational Roles – Identities within ITIM can be grouped by membership to Organizational Roles, or roles. Such Organizational Roles are intended to reflect the roles that exist within an organization that uses ITIM for identity management. Organizational Roles are used by Provisioning Policies to determine which identities shall have accounts on which managed resources. A Provisioning Policy defines a number of services and attributes a user shall have on these services (e.g. membership of groups on the service) and is associated with dedicated Organizational Roles.
  When an identity is added to an Organizational Role, this identity becomes a subject to the Provisioning Policies referring to this role and therefore to the creation (or modification, deletion) of accounts on the services defined within these policies. Granting access to services is referred to as Entitlement.
- ITIM Groups – An identity may be a member of an ITIM Group. Membership in an ITIM Group provides a set of default permissions and operations, as well as views, that group members need. ITIM relies on fine-grained access control performed by evaluating ACIs (Access Control Item, i.e. ITIM-specific access control policies) that delegate specified rights to ITIM Groups.
  In most environments, all identities will be members of at least one ITIM Group that delegates the right to change account passwords via the web-based user interface provided by the ITIM server to its members. The modified password will then be provided by way of connectors to all managed resources the identity has an account on. Only dedicated identities belong to ITIM Groups that delegate the right of system administration or Organizational Role management to these users. Membership to the predefined Administrator group exempts a user from all access control on the ITIM server.
  Note: while ITIM provides the necessary functionality to provision accounts to managed resources, i.e. to provide a service with the necessary information to create an account and to trigger this creation, the enforcement of (security) functionality on the managed resources for such an account is by design left to the managed resource.

TOE Boundary and Runtime Environment

The TOE consists of the ITIM server, which is comprised by the Core Services, Applications and Web User Interface subsystems, and the adapters that provision the managed resources, including the RMI dispatcher add-on for directory integrator-based TIM adapters.

The ITIM server component is completely built on Java related technology; TDI-based adapters are built on Java related technology and the Tivoli Directory Integrator architecture, and ADK-based adapters are implemented in C and C++ utilizing the ADK to communicate with ITIM. Therefore, the runtime environment provided by the IT environment for running the TOE is a Web Application Server (WebSphere) for the ITIM server, Tivoli Directory Integrator (including the necessary connectors) for the Oracle adapter and Windows operating systems for the Active Directory adapter.

The Policy Directory (in fact an LDAP repository), the Workflow, or transaction, data base and the external sources for person information (i.e. the identity stores) are part of the IT environment.

TOE Security Functionality

The TOE provides the following security functionality:

- Auditing of activities
  The TOE is capable of auditing internal events (e.g. the modification of provisioning policies or the creation of new users) by generating audit records for all transactions that are stored in a database provided by the IT environment. The TOE also offers functionality to review these audit records.
- Identification and authentication
  The TOE identifies users (including administrators) by user name and authenticates them by password. ITIM users are persons with an account on the TOE; they can be organized by memberships to ITIM groups.
  The user identities are stored in a directory server provided by the IT environment.
  Only hashes of the passwords are stored in the TOE. Password policies can be applied to enforce requirements on the quality of the password that a user chooses. Lockout mechanisms prevent password guessing attacks.
- Authorization (access control)
  The ITIM server performs authorization for user actions, commonly referred to as requests, based on Access Control Item (ACI). ACIs can be assigned to ITIM groups and ACI principals (e.g. administrators). One pre-defined ITIM group exists for ITIM administrators, other groups can be defined by the customer.
  The TOE offers three groups of ACIs:
    - organizational (access control to functions related to entities within an organization or the organization itself)
    - provisioning (access control to functions related to provisioning and other policies)
    - reporting (access control to functions related to the generation of reports)

  ACIs can be created, modified, or deleted by either a system administrator or explicitly entitled users. Members of the predefined Administrator group are not subject to any access control.

- Provisioning
  Provisioning policies define the services the persons belonging to an organizational role shall have access to. If a person belongs to an organizational role defined within the TOE, and a provisioning policy specifies the entitlement of this organizational role to a certain service, the person is entitled to have an account on this service. Such an account may be created upon user request by interaction with the TOE (if the person belongs to an ITIM group), or it may be manually created by administrator request, or may be automatically created for the person during periodic policy enforcement.
- Service Reconciliation and Identity Feeds
  The TOE provides the capability of gathering account information from managed resources. Reconciliation retrieves and compares user information stored on a managed resource with the corresponding data stored in the ITIM database. Data can be imported via Identity Feeds. For example, user data (e.g. person, or identity information) can be imported into an Organization managed by the TOE.
  This functionality eliminates the need for manual entry of a potentially large number of persons to the TOE's database and allows automated reconciliation with systems used for human resource management within an organization.

Documentation

The evaluated documentation as outlined in table 2 and listed in section 13.1 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.

IT Product Testing

Report on the Developer Testing Effort

Test Configuration

The test configurations used for testing is outlined in "Platforms" sheet of the testmapping document and covers different permutations of:

- Operating systems: Windows 2003 R2 32/64 Bit Kernel, Solaris 10 64 Bit Kernel, Redhat 4 32/64 Bit Kernel, AIX 5.3 64 Bit Kernel, SUSE 10 32Bit Kernel
- WebSphere application server (WAS) version 64bit 6.1, 64bit WAS 6.1 FP9 + PK37456, 64bit WAS 6.1 FP15, 64bit WAS 6.1 FP17, 32bit WAS 6.1, 32bit WAS 6.1 FP5, WAS 6.1 FP9, 32bit WAS 6.1 FP15
- Databases: DB2 9.1, DB2 9.1 FP2, DB2 9.1 FP3, Oracle 10g (10.2.0.1.0), MS SQL Server 2005, MS SQL Server 2005 SP2
- LDAP servers: ITDS 6.0.0.1, ITDS 6.0.0.3, ITDS 6.1, ITDS 6.1 FP1, SunOne 5.2
- Browsers: Internet Explorer 6, IE 6.0 SP1, IE 6.0 SP2, IE 7.0, Firefox 1.5.0.10, FireFox 1.5.0.12, Firefox 2.0.0.4, Mozilla 1.7
- Configuration: single system or systems allocated on several servers

In addition, the adapter test documents outline the configuration needed for testing the adapters. This includes the specification of the software components needed for testing.

These documents also the state which adapter versions have been tested: Windows AD adapter build version 5.0.2 (identical with the release version 5.0.1) and Oracle adapter build version 5.0.001 (identical with the release version 5.0.1).

The evaluator verified that testing covers the different implementations of security functionality offered by the software (storing of TOE data, protection of TOE execution domain, providing of reliable time stamps). Since all different implementations have been sufficiently tested, all software systems defined in the Security Target do not differ in their security functionality.

The evaluator verified also that the only software components that provide security functionality as required by the SFRs for the TOE environment are the WebSphere Application Server, ITDI server, ITDS LDAP server, and RDBMS that interfaces DB2 or and Oracle databases. This is consistent with the assumptions stated in the Security Target about the TOE IT environment.

Conclusion

The evaluator verified that the developer testing was performed on software configurations consistent with the set stated in the Security Target.

The evaluator was able to follow and fully understand the developer testing approach based on the information provided by the developer.

The evaluator analysed the developer testing coverage and depth by reviewing all test cases as demonstrated in the test coverage analysis. The evaluator found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification.

The evaluator reviewed the test results provided by the developer and found them to be consistent with the test plan.

Report on the Evaluator Testing Effort

TOE Test Configuration

The evaluator installed and used Windows 2003 server operating system. The following software has been installed by the evaluator :

- DB2 9.1 FixPack 2
- ITDS 6.1
- WebSphere application server (WAS) 6.1 with FP9
- ITIM server version 5.0 (build 1559 according to the footer shown with the WebGUI)
- IBM Tivoli Directory Integrator Version 6.1.1
  - Windows AD adapter 5.2.3790

The evaluator chose to install and test only the Windows AD adapter. The adapter API of ITIM 5.0 is not changed with respect to ITIM 4.6. In the previously evaluated version of the product both adapters were implemented as local components to ITIM 5.0 exporting the same API. In ITIM 5.0 the adapter API is kept the same but both adapters are now implemented as TDI-based adapters whose interfaces are invoked through Java RMI. The correct functional behavior of the Oracle TDI-based adapter is asserted by the developer test evidence and also by the fact that it is a commercial product used by many ITIM 5.0 customers. Since both adapters depend on the same technology to inter-operate with ITIM 5.0, it is sufficient to test only one of them.

The evaluator installed the software as outlined in the installation guidance for the ITIM 5.0 server as well as for the adapters. After successful installation the evaluator applied the configuration outlined in [9]. Every configuration aspect was covered by the evaluator to bring the system to the evaluated configuration.

Summary of Evaluator Test Results

The evaluator testing effort consisted of two parts: i) a re-run of a subset of the developer test cases; ii) execution of the tests created by the evaluator.

The evaluator performed all tests at the atsec Common Criteria Lab in Austin (Texas, USA) using the selected platforms listed above. All actual test results obtained by the evaluator matched the expected results as documented in the evaluator test descriptions.

Report on the Evaluator Penetration Testing

The evaluator performed the penetration testing on the very same system and configuration used for testing. Therefore, the configuration and installation description given in the previous section above applies.

The evaluator devised the penetration tests by first identifying preconditions that must be met in order to successfully continue and execute a penetration attack. Therefore, if any of the preconditions for the devised test cases showed a negative result (i.e. the test failed showing that the precondition does not hold), the evaluator concluded that further analysis was not necessary as the chosen approach for penetration was invalid.

Summary of the Evaluator Penetration Testing

The evaluator devised a set of penetration tests based on the developer's vulnerability analysis, well-known attacks for the class of products that the TOE represents, and on the evaluator's knowledge of the TOE gained through the evaluation activities.

All penetration tests were based on suspected obvious vulnerabilities. The evaluator conducted those tests and did not find any vulnerability that resulted in a penetration of the TOE with moderate attack potential. Also, the vulnerability analysis did not identify any vulnerability that could be exploited by attackers with moderate attack potential.

Therefore, the evaluator determined that the TOE is resistant against attacks with moderate attack potential.

Evaluated Configuration

This certification covers the following configurations of the TOE:

- Only adapters that are part of the evaluated configuration of the TOE (i.e. the adapters identified in section 2.7 of [6]) are to be used. No other adapters in the IT environment may be connected to the TOE, including LDAP or vendor specific adapters. The adapters that are part of the evaluated configuration use the following protocols for communication with the ITIM server: DAML for the Windows AD adapter, and RMI for the Directory Integrator-based Oracle Database adapter.
- The ITIM server component of the TOE is installed and operated on a dedicated Web Application Server that communicates via network connections with clients, adapters and the resources in the IT environment (e.g. LDAP registry, RDBMS) as supportive to the TOE.

- Tivoli Directory Integrator is installed and operated either on a separate dedicated machine or in the same machine where the ITIM server is hosted; in the former case a secure channel between the servers must be provided by the IT environment (in any case both the TOE and TDI run on separate java runtime environments). The RMI dispatcher add-on (which is part of the TOE) shall also be installed and configured as documented. TDI is expected to be used as a supporting application for the TOE; a dedicated TDI server instance is used exclusively for supporting each of the services implemented through a Directory Integrator-based adapter.
- “Event notifications” of adapters (remote password synchronization) and identity feeds are not supported in the evaluated configuration. Identity feeds are operated by using their reconciliation functionality.
- Only the English user interface (and guidance) is to be used.
- The usage of low-level APIs (as opposed to the exported API) to extend the functionality of the TOE’s Core Services by plugging in user-specific extensions is prohibited.
- The Web Application Server is installed on one dedicated machine that is physically and logically protected. Clustering is disabled.
- The Directory Server and RDBMS are installed either together on one or separated on two systems. They are for dedicated use by the TOE only and configured accordingly (e.g. restricted network availability). The underlying machine(s) are dedicated to run only these applications.
- All network communication is protected, either by cryptographic (SSL / TLS) or organizational (restricted network access) means.
- Access to network sockets opened by adapters for configuration with the agentCfg tool is restricted to “root” users, or administrators, on the local operating system hosting the adapter. High quality passwords must be set for the adapter configuration.
- Single Sign-On is not supported.

The evaluated configuration of the TOE restricts the choice of products that can be selected by the customer to fulfil the dependencies of the ITIM server on its IT environment, such as described in the Security Target [6], chapter 2.8.

Results of the Evaluation

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 class ASE
- All components of the EAL3 package as defined in the CC (see also part C of this report)

- The components ALC_FLR.1 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-0237-2006, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the drop of the conformance claims to the IMPP (Identity Manager Protection Profile); the inclusion of several new TSF interfaces; the adaptation of new versions of adapters, either with more functionality or with a different underlying technology (TDI server); new versions and products as part of the IT environment and new guidance documentation.

The evaluation has confirmed:

- for the Functionality: Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant EAL 3 augmented by ALC_FLR.1
- The following TOE Security Functions fulfil the claimed Strength of Function : moderate F.I&A: – Password policy enforcement

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.

Results of cryptographic assessment

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

Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 and listed in section 13.1 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

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.

Definitions

Acronyms

ACI	Access Control Item
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Errichtungsgesetz
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology

ITIM	IBM Tivoli Identity Manager. Also: TIM
ITSEF	Information Technology Security Evaluation Facility
JMS	Java Messaging Service
LDAP	Lightweight Directory Access Protocol
LDAP v3	LDAP Version 3
PP	Protection Profile
RDBMS	Relational Data Base Management System
RMI	Remote Method Invocation
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SSL	Secure Socket Layer
ST	Security Target
TDI	IBM Tivoli Directory Integrator. Also: ITDI
TIM	IBM Tivoli Identity Manager. Also: ITIM
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
WAS	Web Application Server
XML	Extensible Markup Language

Glossary

Access Control Item Controls user access by defining the access privileges of an ITIM Group or ACI principal. An ACI grants or denies the ability to perform Tivoli Identity Manager functions.

Account Object that represents the information defined for a user, or identity, within the context of a managed resource. This information may be security and/or profile characteristics for the user specific to the resource.

Adapter Software module that is part of ITIM, but distributed remotely from the ITIM server as the part of a connector that interacts directly with the managed resource (service). The module implements the connector commands by translating them in to resource specific commands.

Administrator An ITIM User being member of the Administrator Group. An Administrator is not subject to any access control.

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

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.

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

BPOrganization Business Partner Organization. One of the types of subsidiary entities that can be added to an Organization.

BPPerson Business Partner Person. A Person in a Business Partner Organization.

Business Unit A subsidiary entity of an Organization.

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

Connector Connectors support a specific resource. One element of the connector, the service provider, executes at the ITIM Server machine to cause data to be delivered to the managed resource. The other element of the connector, the adapter, executes at the managed resource. The connector is responsible for receiving directives from the ITIM Server and implementing changes at the managed resource, using the primitives of the managed resource.

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.

Entitlement A construct to define a set of permissions, or privileges, on a managed resource. This construct will be organized into a Provisioning Policy to grant those permissions to a set of identities (represented by roles).

Entity 1) A Person or object for which information is stored. 2) One of the following classes, as referred to by the Tivoli Identity Manager system: Person, BPPerson, Organization, BPOrganization

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

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

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.

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

Identity Feed An automated process in which the Tivoli Identity Manager system imports user data from a human resources database or file and feeds the information into the Tivoli Identity Manager directory.

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.

ITIM Group An ITIM Group delegates management rights to ITIM Users on the ITIM server. Management can be restricted to only change its own password, over being able to manage Organizational Roles and membership of other identities to those roles, up to being allowed to perform system management for the TOE. Adding an identity to at least one ITIM Group implies creation of an account for that identity on the ITIM server.

ITIM User A Person provisioned with an ITIM account, i.e. an account to access the TOE. This requires an entitlement for the Person to the ITIM Service. Users can be delegated (by membership of an ITIM Group) to perform certain management actions within ITIM.

Managed Resource An item that can be owned or accessed by a set of identities. This resource will be represented as a service in ITIM. Provisioning policies will entitle the appropriate identities to ownership of, or access to, a resource. Adapters enforce the entitlements on the resources. Examples of resources are NT domains, SAP systems, RACF systems, mail servers, and databases.

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

Organization A logical construct that stands on the top of an organizational hierarchy (Organization Tree) managed with Tivoli Identity Manager. Generally, an organization represents a company.

Organizational Element Organization, Organizational Unit, Location, Business Partner Organization, or Administrative Domain.

Organizational Role A named set (group) of identities. The determination of which identities should belong to a role is specific to the customer’s business objectives.

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

Orphan Accounts Accounts on a Managed Resource whose owner in the Tivoli Identity Manager system cannot be determined.

Person Object within ITIM representing a human or computing entity that is being managed, or controlled, and audited. Persons can be entitled (by membership of an Organizational Role that is subject to a Provisioning Policy) to use services in the IT environment. In such case of account provisioning, a Person will be represented as a user on a resource. This relationship is modelled in ITIM as a Person owning zero up to many accounts.

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.

Refinement The addition of details to a component.

Relational Data Base Management System ITIM employs a RDBMS in the IT environment as transaction database, which includes storage of audit records.

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 Function Policy The security policy enforced by an SF.

Security objective A statement of intent to counter identified threats and/or satisfy identified organisation security policies and assumptions.

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

Selection The specification of one or more items from a list in a component.

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

Service Object that represents a managed resource that supports actual users. A service is protected via the creation of policies. The user information on the service is represented with accounts. These accounts are updated by ITIM through a connector.

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 resource Anything useable or consumable in the TOE.

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 Functions Interface A set of interfaces, whether interactive (man-machine interface) or programmatic (application programming interface), through which TOE resources are accessed, mediated by the TSF, or information is obtained from the TSF.

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

TOE security policy model A structured representation of the security policy to be enforced by the TOE.

Trusted channel A means by which a TSF and a remote trusted IT product 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 data Data created by and for the user that does not affect the operation of the TSF.

View A set of tasks that a particular type of user can see, but not necessarily perform, on the graphical user interfaces (self service and administrative consoles).

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.[8]

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

[6] Security Target BSI-DSZ-0556-2009, Version 1.12, 10.04.2009, IBM Tivoli Identity Manager 5.0 Security Target, IBM

[7] Evaluation Technical Report, Version 2, 26.05.2009, Evaluation Technical Report, atsec information security GmbH (confidential document)

[8] *Configuration list for the TOE*:
- Configuration lists for design documents, 23.07.2008
- CMVC list for Product documentation, 02.07.2008
- Configuration lists for evaluation specific documents, 23.07.2008
- Security flaw CMVC list, 12.12.2007
- Archive with source code configuration lists, 18.06.2008
- CM-Evidence-tim50-TestProjects-CVS-Log.zip, 07.08.2008
- ITIM_5x_CVT_Execution_DB_IBM_C.pdf, 03.10.2008
- ITIM_5x_SVT_Execution_DB-IBM.pdf, 03.10.2008
- CVT-SVT-TP-SS.JPG, 17.09.2008

Guidance documentation

[9] IBM Tivoli Identity Manager Common Criteria Guide Version 5.0, First Edition (SC23-9978-00), 2009

[10] Guidance [INST], IBM Tivoli Directory Server Version 6.2, What's New for This Release Tivoli Identity Manager Server Version 5.0 Installation and Configuration Guide, First Edition (SC32-1562-00), December 2007

[11] Tivoli Identity Manager Server Version 5.0 Manager Directory Integrator- Based Oracle Database Adapter Installation and Configuration Guide, First Edition (SC23-6157-00), 2007

---

[8] specifically

- AIS1 Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers. Version 13, Stand: 14.08.2008
- AIS14 Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria). Version 4, Stand: 02.04.2007
- AIS23 Zusammentragen von Nachweisen der Entwickler. Version 2, Stand:11.03.2009
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.

[12] Tivoli Identity Manager Server Version 5.0 Manager Manager Active Directory Adapter Installation and Configuration Guide, Version 5 (SC23-6175-00), 2007

[13] IBM Tivoli Directory Server Version 6.2, Programming Reference ITIM Online Help and Information Center, Version 5, http://publib.boulder.ibm.com/infocenter/tivi help/ v2r1/index.jsp?topic=/com.ibm.itim.doc/welcome.htm

[14] IBM Tivoli Identity Manager Version 5 Problem Determination Guide, 2007

[15] Administering, 27.03.2008

[16] Configuring, 27.03.2008

[17] Customer API documentation, Version 5, 15.10.2008

[18] Java Doc API documentation, Version 5, 28.08.2008

This page is intentionally left blank.

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.”

Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.