Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0471-2009

for

Tivoli Provisioning Manager (TPM)
Version 5.1.1.1 Interim Fix 6

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-0471-2009

Provisioning Manager

Tivoli Provisioning Manager (TPM) Version 5.1.1.1 Interim Fix 6

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

Common Criteria
Recognition
Arrangement
for components up to
EAL 4

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, 20 May 2009
For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski L.S.
Head of Department

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

[1] Act 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] [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)

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 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

2.1 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 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.

2.2 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.

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 Tivoli Provisioning Manager (TPM) Version 5.1.1.1 Interim Fix 6 has undergone the certification procedure at BSI.

The evaluation of the product Tivoli Provisioning Manager (TPM) Version 5.1.1.1 Interim Fix 6 was conducted by atsec information security GmbH. The evaluation was completed on 31 March 2009. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: 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.

[6] Information Technology Security Evaluation Facility

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.

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 Tivoli Provisioning Manager (TPM) Version 5.1.1.1 Interim Fix 6 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 Corporation
8200 Warden Ave
Markham, On, Canada
L6G 1C7
Canada

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

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

1 Executive Summary

The Target of Evaluation (TOE) is IBM Tivoli Provisioning Manager Version 5.1.1.1 with Interim Fix 0006. Tivoli Provisioning Manager (TPM) is an automated resource management solution for corporate and Internet enterprises. TPM allows managing an organization's system life cycle by providing a centralized solution to:

- Discover existing assets (so-called endpoints) in the IT infrastructure.
- Schedule the installation of operating systems and application software on these assets.
- Determine configuration settings on the managed systems and bring them into compliance with centrally managed policies.
- Install software patches and upgrades on managed machines. Tivoli Provisioning Manager manages a virtual representation of the physical and logical assets in an enterprise's IT infrastructure in a data model, which is stored in the TPM Database. Each asset is represented by a data object. TPM records the changes made to the data objects and for some assets, the data model stores data about the asset and data about deploying or provisioning the asset separately to provide a range of implementation options. In addition, TPM allows grouping of data objects.

In order to limit the ability of performing central management tasks to authorized personnel, TPM provides access control functionality, as well as an auditing mechanism to provide for accountability.

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 5.2. 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
Instance Level Security (F.DAC)	The TOE enforces the Instance Level Security DAC policy for administrators using the TOE interfaces to manage data objects and to execute workflows.
Auditing (F.AUD)	The TOE generates audit records for certain transactions. Facilities to search and review audit records are offered by the TOE's GUI.
Management (F.MGMT)	The TOE offers a web-based GUI for management of the TSF.The management options offered by the GUI depend on the security

TOE Security Function	Addressed issue
	roles that have been defined for the user

Table 1: TOE Security Functions

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

The strength of function claim is not applicable since no TOE security function is based on permutational or probabilistic mechanisms.

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], chapters 3.1, 3.2 and 3.3.

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

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:

Tivoli Provisioning Manager (TPM) Version 5.1.1.1 Interim Fix 6

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Tivoli Provisioning Manager Version 5.1.1		electronic download or on CD media pack
2	SW	Tivoli Provisioning Manager Fix Pack 5.1.1-TIV-TPM-FP0001		electronic download
3	SW	Tivoli Provisioning Manager Interim Fix 5.1.1.1-TIV-TPM-IF00006		electronic download
4	DOC	Common Criteria Guide for Tivoli Provisioning Manager 5.1.1.1, Interim Fix 00006	1.0, 2008-12-05	Delivered with Tivoli Provisioning Manager Version 5.1.1
5	DOC	Tivoli Provisioning Manager 5.1.1.1, readme file for UNIX or Linux	2008-03-05	Delivered with Tivoli Provisioning Manager Version 5.1.1
6	DOC	Tivoli Provisioning Manager 5.1.1.1 IF00006 README	2008-10-24	Delivered with Tivoli Provisioning Manager Version 5.1.1
7	DOC	Tivoli Provisioning Manager 5.1.1.0 Information Center standalone	5.1.1.0, 2007-12	Delivered with Tivoli Provisioning Manager Version 5.1.1
8	DOC	Tivoli Provisioning Manager Installation Guide for AIX	SC32-2234-03, 2007-12	Delivered with Tivoli Provisioning Manager Version 5.1.1

No	Type	Identifier	Release	Form of Delivery
9	DOC	Tivoli Provisioning Manager Installation Guide for Linux	SC32-2233-03, 2007-12	Delivered with Tivoli Provisioning Manager Version 5.1.1
10	DOC	Tivoli Provisioning Manager Installation Guide for Solaris	SC32-2235-03, 2007-12	Delivered with Tivoli Provisioning Manager Version 5.1.1
11	DOC	Tivoli Provisioning Manager Installation Guide for Windows	SC32-2232-03, 2007-12	Delivered with Tivoli Provisioning Manager Version 5.1.1

Table 2: Deliverables of the TOE

No hardware is delivered as part of the product.

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:

- Instance Level Security Policy:
  The TOE implements an access control policy between subjects and objects. The subjects are users. The objects are data objects and workflow attributes. Access to objects by subjects will be mediated by this policy to insure that subjects are only able to gain access to authorized objects.

Details can be found in the Security Target [6], chapter 6.1.1.

4 Assumptions and Clarification of Scope

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

- It is assumed that the machine(s) providing the runtime environment for the TOE are protected against unauthorized physical access and modification.
- The administrators of the TOE, of the TOE's underlying systems, and of the systems in the TOE's IT environment who are involved in safeguarding TSF data or providing functionality that the TOE depends on are assumed not to be careless, willfully negligent, or hostile. They will follow and abide by the instructions provided in the administrator guidance that is part of the TOE. They are well trained to securely and trustworthy administer all aspects of the TOE operation.
- The machines providing the runtime environment for the Provisioning Server are assumed to be used solely for this purpose and not to run other application software except as required for the support of the TOE and for the management and maintenance of the underlying system and hardware. Especially it is assumed that the underlying systems are configured in a way that prevents unauthorized access to security functions provided by or protected by the runtime environment either locally or via any network based connections.
- It is assumed that the TOE is configured and operated in its evaluated configuration.

Details can be found in the Security Target [6], chapter 3.2.

5 Architectural Information

The target of evaluation is IBM Tivoli Provisioning Manager Version 5.1.1.1 with Interim Fix 0006. Tivoli Provisioning Manager (TPM) is an automated resource management solution for corporate and Internet enterprises. TPM allows managing an organization's system life cycle by providing a centralized solution to:

- Discover existing assets (so-called endpoints) in the IT infrastructure.
- Schedule the installation of operating systems and application software on these assets.
- Determine configuration settings on the managed systems and bring them into compliance with centrally managed policies.
- Install software patches and upgrades on managed machines. Tivoli Provisioning Manager manages a virtual representation of the physical and logical assets in an enterprise's IT infrastructure in a data model, which is stored in the TPM Database. Each asset is represented by a data object. TPM records the changes made to the data objects and for some assets, the data model stores data about the asset and data about deploying or provisioning the asset separately to provide a range of implementation options. In addition, TPM allows grouping of data objects.

TPM provides execution of workflows that automate the configuration and allocation of IT assets.

TPM integrates the Tivoli Common Agent Services (CAS), a platform that provides a central agent infrastructure that can be shared by multiple distributed management services. On endpoints, a common agent is installed that communicates with the deployment infrastructure and the provisioning server, and executes the tasks that have been scheduled on the TPM server.

The TOE provides a web-based graphical user interface (GUI) centralizing all administration and management tasks for the TOE. A programmatic web services (SOAP) interface is also provided that can be accessed by users directly or via administrative tools provided with the TOE. In addition, local command line interfaces (CLI) are provided for administration tasks on the server. Remote CLIs make use of the SOAP interface.

TPM is a software-only product. The evaluation includes the installation of the TOE as delivered on CD-ROM media pack or as an electronic download via a secure IBM site. The TOE distribution includes the TOE itself, WebSphere Application Server, DB2 database, and IBM Tivoli Directory Server, of which the latter three components are considered part of the TOE environment. The TOE environment also includes the respective operating systems as specified in the ST and the Java Runtime Environment.

The TOE is a J2EE application running on an application server, i.e., IBM WebSphere Application Server (WAS), thus relying heavily on the security mechanisms provided by WAS including authentication of users, role-based security for user interfaces, and secure communication via SSL/TLS or OpenSSH between the TOE parts as well as the TOE and its environment; i.e., network connections between the server, the deployment infrastructure, and the endpoints. Moreover, since the TOE's runtime environment is the Java Runtime Environment and additional services implemented in Java, there is no direct dependency of the TOE on the operating system (or the hardware) that the runtime environment runs on. The Java-based runtime environment provides a complete abstraction layer.

Major structural units of the TOE

The TOE consists mainly of the provisioning server and the endpoints. The provisioning server provides functionality to users, while the endpoints are remote resources managed with TPM.

The provisioning server itself is structured into a number of subsystems, which are described in detail in the high-level design of the TOE. The subsystems are as follows:

Data Center Model (DCM) Subsystem:
This subsystem is essentially implemented as a relational database that provides a centralized repository represented by an object model containing the physical and logical assets that TPM manages. The DCM captures and maintains all the relationships of these assets. DCM treats physical assets as DCM objects, and access to these objects is subject to access control mechanisms provided by the DCM. From a security perspective, the DCM subsystem provides role-based and instance level security authorization as access control mechanisms and audit functionality, including recording an audit trail for security-relevant auditable events.

Reporting Subsystem:
This subsystem provides functions for the retrieval of current information about enterprise inventory, activity, system compliance, and audit records. This subsystem works together with the DCM subsystem to implement the audit system. Reporting mainly is responsible for making audit records available for search and select operations.

GUI Subsystem:
This subsystem provides the main interface to users to access the TOE. The interfaces are provided as Web-based operator and administrator consoles for users/administrators to interact with the TPM server. It directly or indirectly enforces authentication of users, authorization of access to data, and management of data by invoking other respective subsystems. Using this interface, the administrator can manage user account security attributes related to Role-based Security policy as well as Instance Level Security Policy attributes, defining workflows including assigning required permissions to workflow parameters, and audit enablement and records.

Web Services Subsystem:
This subsystem is implemented as a self-contained application that allows computers in a network to connect dynamically via standard network protocols such as HTTP, and run transactions in real time to manage and configure the environment of TPM. This subsystem provides interfaces for users to access the TOE directly or via administrative tools to perform administrative tasks such as changing the operating modes, managing failed servers or running workflows. Web Services are provided programmatic web services (SOAP) interfaces.

Deployment Interface Subsystem:
This subsystem provides deployment services, such as provisioning-related information to other components of TPM including the deployment engine and deployment infrastructure.

Deployment Engine Subsystem:
This subsystem is responsible for creating, storing, and running repeatable workflows that automate the configuration and allocation of IT assets. It is also responsible for executing workflows and interacting with the DCM subsystem to enforce access control on the workflows.

Deployment Infrastructure Subsystem:
This subsystem implements the scalable infrastructure managing large distributed environments.

Discovery Subsystem:
This subsystem provides a way to discover new devices and configuration changes for managed resources (e.g., computers, switches, subnets, software and images).

Common Agent Subsystem:
This subsystem is used for managing software distribution and configuration compliance. It collects data from and performs operations on managed resources on behalf of a specified Tivoli management application.

Security Functions:
The security functions of the TOE defined in the Security Target [6] are as follows:

- Instance level security
- Auditing
- Security management

Instance level security:
The TOE offers a pre-defined list of instance permissions that can be granted to users in order to protect individual data objects (assets) from unauthorized access. These individual permissions can be combined into permission groups.

Administrators can define access groups that comprise a set of data objects. Access groups can contain individual data objects, groups, resource pools and application tiers. Permission groups can then be assigned to access groups, and eventually users can be associated with these permission groups within an access group, defining which permissions the user has on the associated objects. The result is a tuple (access group:permission group:user).

The IT environment (via the enforcement of role-based security) determines who is authorized to edit access and permission groups. By default, the authorized users are those assigned to the System Administrator role and superusers, who are not under role-based access control.

When a user requests an operation on a specific data object via one of the administrative interfaces provided by the TOE, access is granted only if one of the specified permissions allow the requested operation type on the specific data object.

Instance level security can also be applied to workflows when configured by administrators. If a workflow definition requires a specific permission for a workflow parameter, TPM will verify that a user has the correct permission for the object that she or he assigned as value for the protected parameter when initiating the workflow.

Users are assigned a default access group upon creation. When a user creates new data objects through the GUI, these objects are added automatically to this access group. Users who have the superuser attribute set in their account are exempt from any access control enforcement.

Audit:
The TOE provides generation of audit records for certain security-relevant events which includes the following:

- auditing of changes to the system configuration including each change to any of the tables in the TPM DB, including all objects in the data model
- user management and access control management including management of users and properties for the access control mechanisms that are stored in the user registry
- user logon/logout

The GUI provides several views that administrators can use to search for and review audit records, as well as to delete audit records that are older than a certain date. Additionally, auditing can be turned on or off on a global basis by Superusers or administrators with the System Administrator role.

Security Management:
TPM provides management capabilities for its security functions and some of the environment-provided security functionality via its user interfaces:

- user management including add, change properties, or delete
- management of access control such as security roles, access groups, permission groups, etc.
- enabling/disabling of the audit system

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

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

7 IT Product Testing

Developer Testing

Test configuration:
The developer's test environment for the TOE is comprised of the systems listed in [6] as part of the evaluated configuration, plus some extra machines that were not relevant due to not being part of the evaluated configuration. For example, Microsoft Windows XP Professional SP2 was used as one of the endpoints.

Testing of the provisioning server components was performed mainly on Microsoft Windows 2003 Enterprise Edition SP2 and UNIX platforms specified in the ST, which also provides the definition of the underlying software:

- IBM WebSphere Application Server 6.0.2 with refresh pack 2, interim fix pack 11, and patch 5.1.1.1-TIV-TPM-IF00006-LA0001
- IBM DB2 Universal Database Enterprise Server Edition 8.2, Fix Pack 11 on Windows
- IBM Tivoli Directory Server 6.0 Fix Pack 1 and/or Microsoft Active Directory
- Java Runtime Environment version 1.4.2
- Cygwin version 1.5.10

As the server components of the TOE rely on the underlying Java layer as the abstract machine, there is no dependency on the real hardware.

Conclusions:
The evaluator has verified that developer testing was performed on hardware conformant to the Security Target. The evaluator was able to follow and fully understand the developer's testing approach by using the information provided by the developer. The evaluator analyzed the developer's coverage and depth of testing by examining all test cases provided by the developer. The evaluator determined that the testing of the TSF was extensive and covered the TSFI as identified in the functional specification.

The evaluator reviewed the test results provided by the developer and concluded that they were consistent with the test plan.

Evaluator Testing effort

Test effort:
In order to gain sufficiency in the developer's testing, the evaluator took the effort to repeat all of the developer's tests. In additional to functional testing, all major aspects of security functionality of the TOE were covered, including access control, auditing, and security management. Penetration tests derived from the vulnerability analysis as well as other evaluation evidence were also conducted.

Test configuration:
The evaluator used the following systems for independent testing:

- For the system that the TPM server runs on, the evaluator used a Windows Server 2003 SE system running on an IBM-compatible PC.
- For the system that the endpoint is installed on, and that the depot server and remote server run on, the evaluator used a Windows XP Professional SP2 system running on an Intel-based IBM ThinkPad laptop.

Evaluator Penetration Testing

Test approach:
The evaluator performed her own vulnerability analysis, taking into account any publicly known vulnerabilities and any potential vulnerabilities identified and reported in the individual evaluation reports during the evaluation.

The evaluator identified several potential vulnerabilities that could be possibly be exploited in the intended environment of the TOE. Hence, the evaluator derived and performed a number of tests to verify whether these vulnerabilities could be used to penetrate the TSF as defined in the Security Target.

Penetration testing is to be performed based on the developer’s vulnerability analysis provided in [9], as well as the vulnerability analysis performed by the evaluator. The evaluator examined the justifications for non-exploitability of the potential vulnerabilities identified by the developer, and came to the conclusion that those justifications are adequate with the exception of the potential vulnerability regarding user input handling.

In addition, the evaluator took into consideration common methods of attacking web-based applications (e.g., port scan attack) that were absent from the developer testing and would provide the evaluator with additional assurance.

Test results:
The result of the penetration testing can be summarized as follows:The evaluator checked for some hypothetical vulnerabilities using penetration testing and vulnerability analysis

techniques. The evaluator did not find as a result of her penetration testing any obvious vulnerability of the TOE that is easy to exploit in the intended TOE environment.

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

- Access control must be enabled.
- The Cascading rules feature must not be enabled.
- The tioadmin user must use the Korn or Bash shell.
- Auditing must be enabled.

9 Results of the Evaluation

9.1 CC specific results

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

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

- All components of the class ASE
- All components of the EAL 3 package as defined in the CC (see also part C of this report)
- The component ALC_FLR.1 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: none
- for the Functionality: Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 3 augmented by
  ALC_FLR.1

A strength of function claim is not applicable since no TOE security function is based on a permutational or probabilistic mechanism.

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

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Errichtungsgesetz
CAS	Tivoli Common Agent Services
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CLI	Command Line Interfaces
DCM	Data Center Model
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
J2EE	Java 2 Platform, Enterprise Edition
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOAP	Simple Object Access Protocol
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TPM	Tivoli Provisioning Manager (the TOE)
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
WAS	WebSphere Application Server

12.2 Glossary

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

Data model - A database, containing physical and logical assets that Tivoli Provisioning Manager manages, their relationships, workflows, et al. The data model tracks IT assets, software, systems and their configuration, each asset being represented by a data object.

Data object - A data object describes a managed asset in the data model.This is the virtual representation of an endpoint in the IT environment. Users can manage these objects and are restricted in their access to them by the Instance Level Security Policy implemented by the TOE. A data object follows a pre-defined structure and is represented by an entry in one of the TPM DB's tables.

Endpoint - The system that is the final destination of a management operation, i.e., the remote resources managed with TPM.

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

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

Informal - Expressed in natural language.

Instance - An individual endpoint managed by TPM. Represented in the data model as a Data object.

Instance Level Security Policy - The Instance Level Security Policy is the DAC policy enforced by the TOE, mandating access of users to the individual data objects in the data model.

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

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

Provisioning Server - The system hosting the central, security-enforcing parts of the TOE, like the administrative interfaces and deployment engine, including the underlying J2EE application server, operating system and hardware.

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.

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.

TPM DB - The database in the IT environment that the TOE uses to store the data model.

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 - Humans or machines interacting with the TOE via the provided user and programmatic interfaces. The term user in this document includes administrators of the TOE unless a specific distinction is made in the text.

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.[8]

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

[6] Security Target BSI-DSZ-CC-0471, Version 1.7, 18.12.2008, Tivoli Provisioning Manager Security Target, IBM Corporation

[7] Evaluation Technical Report, 2.0, 20.03.2009, atsec information security GmbH (confidential document)

[8] Configuration list for the TOE (confidential document):
Configuration item lists for product guidance, March 24, 2008
Configuration item lists for items in TPM2007 LotusNotes DB, Version 1.0, December 2, 2008
Configuration item list for Automation Packages module, March 3, 2008
Configuration item lists for test docs, December 15, 2008
Configuration item list for CI_TI or Topology, Installer module, March 3, 2008
Configuration item list for TPM module, March 3, 2008

[9] Vulnerability Analysis for IBM TPM 5.1.1.1 (with Interim Fix 6), Version 1.2, December 2, 2008

Guidance documentation for the TOE:

[11] Common Criteria Guide for Tivoli Provisioning Manager 5.1.1.1, Interim Fix 00006, Version 1.0, December 15, 2008

[12] Tivoli Provisioning Manager 5.1.1.1, readme file for UNIX or Linux, March 5, 2008

[13] Tivoli Provisioning Manager 5.1.1.1, readme file for Windows, March 5, 2008

[14] Tivoli Provisioning Manager 5.1.1.1 IF00006, README, October 24, 2008

[15] Tivoli Provisioning Manager 5.1.1 Information Center standalone, Version 5.1.1.0, December 2007

[16] Tivoli Provisioning Manager 5.1.1 Installation Guide for AIX, SC32-2234-03, December 2007

[17] Tivoli Provisioning Manager 5.1.1 Installation Guide for Linux, SC32-2233-03, December 2007

[18] Tivoli Provisioning Manager 5.1.1 Installation Guide for Solaris, SC32-2235-03, December 2007

---

[8] specifically

- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.

[19] Tivoli Provisioning Manager 5.1.1 Installation Guide for Windows, SC32-2232-03, December 2007

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.

This page is intentionally left blank.