Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0839-2013

for

Tivoli Security Policy Manager, Version 7.1

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-0839-2013

Access Control System

Tivoli Security Policy Manager
Version 7.1

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

Common Criteria
Recognition
Arrangement

Common Criteria

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

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

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

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

Bonn, 16 December 2013
For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

SOGIS Recognition
Agreement

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

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

2 Recognition Agreements

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

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

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

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

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

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

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

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

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

2.2 International Recognition of CC – Certificates (CCRA)

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

As of September 2011 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 website: http://www.commoncriteriaportal.org.

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

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 Security Policy Manager, Version 7.1 has undergone the certification procedure at BSI.

The evaluation of the product Tivoli Security Policy Manager, Version 7.1 was conducted by atsec information security GmbH. The evaluation was completed on 15 November 2013. 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.

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,

[6] Information Technology Security Evaluation Facility

- the product is operated in the environment described, as specified in the following report and in the Security Target.

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

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

In 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 Security Policy Manager, Version 7.1 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] IBM Corporation
11501 Burnet RD
Austin,TX 78758-3400
USA

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 Security Policy Manager Version 7.1 with the elements IBM Tivoli Security Policy Manager Version 7.1, Fix Pack 4 and APAR IV44553. The TOE controls access to Web Services by defining and enforcing security policies.

Web Service requests are access controlled by the TOE on the WebSphere Application host on which the Web Service is deployed. The request is evaluated against a set of policies based on the XACML v2 standard. Only on a Grant access decision, the request gets forwarded to the targeted Web Service. The policies are centrally managed (e.g. authoring, configuration, and distribution) from the TSPM Management Console which provides an administration interface to the TSPM Policy Server, the actual management server.

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 2 augmented by ALC_FLR.3.

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

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

TOE Security Functionality	Addressed issue
Audit Services	The TOE is capable of auditing internal events by generating audit information that is stored in files protected by the IT environment.
User Data Protection	The TSF implements a rule-based access control mechanism to control access to TSPM management functions to authorized administrative users. The TSF implements a policy-based access control mechanism to control access to the Web Services protected by the TOE. These authorization policies contain custom application roles assigned to Web Services users and groups as well as rules defined by the policy that may be specific to each installation.
Security Management	The central management of the TOE's security relevant parameters is performed remotely by an authorized administrator. The following management functions are available to administrative users: ● Policy Administration ● Rule Parameter Administration ● Classification[8] Administration ● Distribution Target Administration

[8] Here, a classification is a named group of policies that apply to each web service that underlies this classification.

TOE Security Functionality	Addressed issue
	● Application Role Administration ● Service Administration ● User Registry Administration ● Administrative Role Administration ● Policy Operations Administration ● General Administration ● Obligations Administration

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapters 3.1, 3.2 and 3.3.

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

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

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

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

Tivoli Security Policy Manager, Version 7.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Tivoli Security Policy Manager SHA256: CZX6XML.zip: 13ddf95d95a49f0017f00f5d29614da207210c59bdb8775d39b5b1a99921b104 CZX6YML.zip: 14e009af2e0306f484702f69979d9563289ea4b35ad3d64ee63594d240fa370e CZX6ZML.zip: c3b229170e1de53a64c37e7b9a3b3148099fe29f5e4e82e0e8123ea8d4f40740	7.1	Secure Download
2	SW	Fix Pack 4 SHA256: 7.1.0-TIV-ITRTSS-FP0004.zip: f1c1061b2553ea9f4787a61cc26af66fa20c49feb16dd36fc3a58cfb11ba2ee4 7.1.0-TIV-ITSPM-FP0004.zip: 141e970a75b2da68430f084f654943f3ce2bef43cb7a0704dc1481e6c74fe671	FP4	Secure Download

No	Type	Identifier	Release	Form of Delivery
3	SW	APAR IV44553 SHA256: com.ibm.tspm.server.ear: 9abb16f2e80cfa0fdd7376b1da9626d03fe62f91b23f062d39bdba1f8067a52c	IV44553	Secure Download (via support contact)
4	DOC	Security Policy Manager Version 7.1.0.4 Common Criteria Guide [8] SHA256: ac5fc4989222f893ecf79e5602bf033c9180769044e29e017bfdbaa8f21892e1	SC27-5627-00	Secure Download
5	DOC	Security Policy Manager Version 7.1 Administration Guide [9] SHA256: 0416ede7790da206b0fa897b35a84193e3f37444a07cb142255451af52bb2eea	SC23-9476-01	Secure Download
6	DOC	Security Policy Manager Version 7.1 Configuration Guide [10] SHA256: 26aa0df68e8961e373b2768d6c5be99a7c6eb5e24f5e03199444b9807a9bb1c5	GC27-2713-00	Secure Download
7	DOC	Security Policy Manager Version 7.1 Installation Guide [11] SHA256: 638335e4bfe0b4948459f799ff0d55d54ba31b69c8e10eb2deb1e4f127182338	GC27-2712-00	Secure Download
8	DOC	Security Policy Manager Version 7.1 Troubleshooting Guide [12] SHA256: 5f56d216a6b294d7b9ccb4653d79784e64ea6d134c1ad3375645bdbe819340bb	GC27-2711-00	Secure Download
9	DOC	Security Policy Manager Version 7.1 Error Message Reference [13] SHA256: 2c42a856f089bdc43b201fa5b01a673c83cbae5afd2209ea8c3cac40bc52b4e5	GC23-9477-01	Secure Download
10	DOC	TSPM Online Fix Pack 4 Guidance [14]	None	Online

Table 2: Deliverables of the TOE

2.1 Overview of Delivery Procedure

The TOE base release, its associated fix pack, and the required APAR fix are all provided via online delivery. The TOE base is available from IBM Passport Advantage (http://www.ibm.com/software/passportadvantage/) while the fix pack is accessible from IBM Fix Central (http://www-933.ibm.com/support/fixcentral/). In both cases, the Download Director applet provides for a secure download. The APAR fix is obtained via sftp (Secure FTP), details of which are provided to the TOE end user by IBM customer support.

The guidance is provided on the IBM support page (http://www.ibm.com/support) by clicking the Documentation tab and then performing a search using the TOE's guidance serial number. This download method also uses the Download Director applet for secure delivery. The Common Criteria Guide itself contains details on the secure delivery for the TOE components mentioned above.

2.2 Identification of the TOE by the User

The user identifies the TOE and the fix pack by using the product selection option including the TOE type, name, version, and platform as explained in the Common Criteria Guide.

The documents are labelled with the product, document and version numbers as indicated in table 2 above and can be checked by the users installing the system. In addition the user must verify the integrity of the TOE parts by checking the hash values listed in table 2 with a eligible checksum utility.

The TOE reference of the installed TOE can be verified by the administrator through an combination of checks depending on the component to be verified:

- looking up the information in special version information files on the server,
- through the TOE version web page or
- by performing SHA-1 checks of the patched binary files.

The Common Criteria Guide contains details on how to identify and verify each component.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: The TOE is a security policy manager and its main purpose is therefore to provide audit functionality, user data protection and security management.

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:

- The runtime environment for the TOE must be able to securely transfer data between the servers and clients that comprise the TOE, and between data sources in the operational environment.
- The runtime environment for the TOE shall implement authentication mechanisms commensurate with the level of protection sought by the TOE, and provide authentication decisions for TOE users to the TSF.
- The runtime environment shall provide a reliable time source for the TOE’s use.
- Those responsible for the operation of the TOE must ensure that administrators are not careless, wilfully negligent, or hostile, and that they are well trained and will follow the provided administrator guidance to install, configure and operate the TOE and the TOE environment. This includes ensuring that all access credentials are protected against disclosure by the users of the TOE, and that only trusted authentication providers are used.
- Those responsible for the operation of the TOE must ensure that the systems hosting the TSPM Administrative Console, TSPM Server, and RTSS Server components are used solely for this purpose and configured in a way that prevents unauthorized access to the TOE and any TSF and user data, including audit records generated by the TSF.
- The environment provides physical security commensurate with the value of the TOE and the data it contains.
- The runtime environment provides the following support for the TOE:
  - Identification, authentication, user-subject binding, rule-based access control, and GUI rendering support for administrative users accessing the TIP Management Console,
  - Identification, authentication and user-subject binding of application users for the RTSS Client,

- Audit support, including audit record formatting, timestamp, and storage.

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

5 Architectural Information

The architecture evolves around the design pattern of an enforcement point (PEP), a decision point (PDP) that is asked for a decision by the PEP, and an administration point (PAP) as follows:

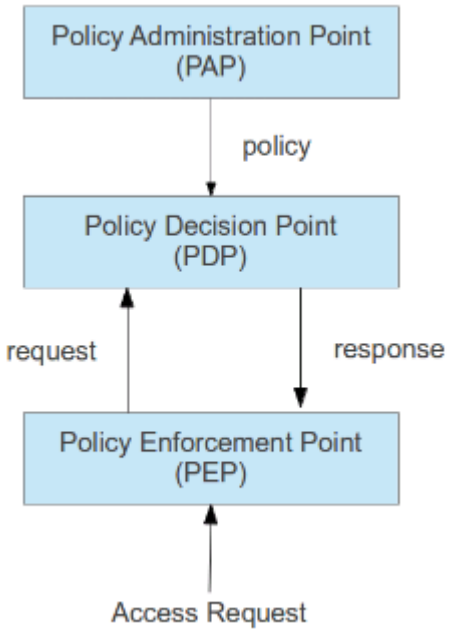

Figure 1: Abstract Core Components

This abstract architecture is mapped to the TOE components as follows:

- PEP: Runtime Security Services (RTSS) Client
- PDP: Runtime Security Services (RTSS) Server
- PAP: TSPM Policy Server

In addition, there is another component called TSPM Management Console which provides a graphical front end to the TSPM Server.

All components are deployed in their own server machine (with exception of the console which is hosted on the same machine than the TSPM server), and communicate with each other over the network.

Runtime Security Services (RTSS) Client

Tivoli Security Policy Manager (TSPM) RTSS Client consists of one J2EE application that runs in WebSphere Application server and acts as a PEP. Its tasks in the general process of an access request are to receive the request, to notify the RTSS Server of the request, receive the RTSS Server's decision response, and finally to enforce the decision by either permit or grant access to the requested Web Service.

Runtime Security Services (RTSS) Server

Tivoli Security Policy Manager (TSPM) RTSS Server consists of one J2EE application that runs inside the WebSphere Application Server (WAS) container. It acts as a Policy Decision Point (PDP), and a Policy Distribution Target (it collects policies that are sent to it for later evaluation process). As part of the request evaluation, it evaluates a request against the applicable policies, and provides a result of either grant or deny.

TSPM Policy Server

The TSPM Policy Server implements the management functionality, e.g., to create, modify, or delete policies, service definitions, and administrative users. It acts as a Policy Administration Point (PAP) and distributes policies to the PDP.

The TSPM Management Console

The TSPM Management Console is the primary management interface for the TOE, which administrators use to manage the TSPM Policy Server components.

Although the administration contains the definition of administrators, roles, and permissions, the TOE itself does not implement authentication services. Instead, each component is integrated into an Web Application Server such that only authenticated users can use the TOE management functionality, and that all transmitted data is encrypted (part of the TOE environment).

6 Documentation

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

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

7 IT Product Testing

7.1 Developer Testing

Test Configuration

The test environment contains three machines with Red Hat Enterprise Linux 5.5 and the

WebSphere Application Server 7.0. The following roles are assigned to the machines and

comprising the TOE:

- Machine 1: TSPM Server as policy administration point and TSPM Management Console to manage the TSPM Server
- Machine 2: RTSS Server as policy distribution target and policy decision point
- Machine 3: RTSS Client as policy enforcement point

Additionally the test configuration on machine 1 requires a user registry, in this case the Tivoli Directory Server 6.2, Tivoli Integrated Portal 1.1 and DB2 9.5 as a policy database.

The test suite consists of manual test cases which have no ordering dependencies so they can be executed without following a specific order.

Each test case of the test environment requests a special set of ldap-users, which are assigned to a specific group called "cc_group".

As the TOE states conformance to the XACML 2.0 standard the developer runs the "XACML Version 2.0 Conformance Tests" which are described at https://www.oasis-open.org/committees/download.php/14877/.

Test Approach

The developer tests comprise of two test suites:

Manual tests on the TSFI

All manual test cases are following the same testing approach. First all pre-conditions are defined for the test. Those are for example:

- A list of users that have to be created,
- a list of groups the users should be assigned to and
- a description which roles are needed for the test.

After all pre-requisites have been set, the test case description shows a bullet list of all actions that have to be performed to pass the test. Those are for example:

1. Login to TSPM with one of the specified user,
2. perform the prior specified action that should be allowed and
3. another action that should not be possible with the assigned permissions of the user.

The manual tests contains two different types of test cases. On the one hand there are "Portal Test Cases" that require that a group is created and users are added to that group. The objective of those test cases is, whether the user can only perform actions, he has the permission to. On the other hand there is one "Authorization Test Case" that checks whether the policies of the TSPM Server are used for the authorization decision of the RTSS Client. This authorization test is not performed by using the portal web interface of the TSPM Management Console (as for the portal test cases), but is executed using the web service interface of the RTSS client machine.

Automated tests of the internal XACML component

The additional XACML test suite contains a set of categorized test cases. Each test case consists of the following files:

*Request.xml	This file contains the input for the test suite.
*Policy.xml	This file contains the policies for the access/decline decision
*Response.xml	This file contains the expected result. Only if its content is semantically consistent with the actual result, the test succeeded.

Result Documentation

The expected results of each test case is documented in the test case description itself. The actual result is part of the result file that is created manually by the tester for each test run. Each result file contains an amount of results, one per sub test that has to match with the expected result of the test case description to pass the overall test successfully.

The expected results of the XACML tests are stored in the *Response files as explained above.

Test Coverage

The functional specification has identified the following TSFI:

- TSPM Management Console - Accessed via a browser by the administrator
- TSPM RTSS JAX-WS PEP HANDLER - Handles the web service interface on the RTSS client machine where the access request arrives

The TSFI "TSPM Management Console" is covered by the "Portal Test Cases" and the "TSPM RTSS JAX-WS PEP HANDLER" by the "Authorization Test Cases". Each test case description consists of a list of all SFRs that are covered by the test case.

The XACML tests are additional tests for the TSPM RTSS JAX-WS PEP HANDLER.

Conclusion

The evaluator has verified that the developer testing was performed in a test environment which is conformant to the Security Target.

The evaluator was able to follow and fully understand the developer testing approach by using the information provided by the developer and viewing the testing during a web conference with the developer test team.

The evaluator analysed the developer testing coverage of the testing by reviewing all test cases.

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

7.2 Evaluator Independent Testing

Test Configuration

The evaluator's test configuration was the same as the developer's test configuration, but newer versions of the Directory Server (v6.3) and DB2 (v9.7) were used. The setup and configuration was performed in accordance to the evaluated configuration described in the guidance.

Test Effort

The evaluator chose 4 of the 17 developer test cases to be executed on the developer test system. For each of the these tests, some modifications in the test procedure were demanded as test variations.

The evaluator devised and performed 10 own independent test cases, where one is an automated test.

Most of the tests use the Web Service interface and the Management Console interface. For the Web Service interface, several variants of Web Service clients have been created.

Test Approach and Depth

The evaluator witnessed the developer testing via a web conference, where a subset of the developer tests were executed based on the evaluator's choice could be observed. Finally, modifications were made to observe respective failures to occur in the tests, thereby verifying that the developer test framework properly catches and displays test failures.

The evaluator tests were devised to test the TOE in the following areas (the respective security functions are listed in brackets):

- Central management of distributed components (Security Audit, Security Management)

- TOE service classification (Security Management)
- Extended policy configuration operations, making more use of different types of policy rule parameters (RTSS Access Control)
- TSPM server authorization enforcement (TSPM Management Console Access Control / EJB)

For the last point above, the evaluator was using an internal interface to exercise the TSPM server directly instead of using the externally visible management Web GUI.

Test Results

All tests of the evaluated functions have been performed successfully.

7.3 Evaluator Penetration Testing

Test Configuration

The tests were performed on the TOE that was installed on the only supported WebSphere Application Server 7.0 on a RHEL 5.5 64-bit platform. The test configuration in terms of the evaluated configuration settings and software versions was the same than for the evaluator's independent testing (following the evaluated configuration defined in the CC-specific guidance provided by the developer).

Test Effort, Approach and Depth

The evaluator used the CVE, Google, IBM support page, and IBM incident response page for finding publicly documented vulnerabilities. No testable concerns lead to any independent tests based on this search.

The test approach was generally aiming at authorization functions of the TOE, specifically the core function of authorizing access to Web Services. This has been performed through either attempting to gain access to TOE interfaces that should not be externally accessible, or accessing functions with unauthorized web service or TOE users.

The test depths was to not only test the externally visible interfaces, but also by affecting/stimulating the internal interfaces of the TOE. This has been achieved by either preventing the data flow to internal components as mentioned above, or by corrupting key files that are used in the internal communication between distributed TOE components (FDP_EXTACC.1(1), FDP_EXTACF.1(1)).

8 Evaluated Configuration

This certification covers the following configurations of the TOE: The evaluated configuration of the TOE consists of the Tivoli Security Policy Manager version 7.1.0.4 (Fix Pack 4) and the APAR fix IV44553.

The operational environment includes:

- Red Hat Enterprise Linux 5.5 Operating System (64-bit)
- IBM WebSphere Application Server Version 7.0
- IBM Tivoli Integrated Portal Version 1.1 (TIPv1.1) including the internal component TCR for generating reports
- IBM DB2® Workgroup Server Edition Version 9.5 or above

- IBM Tivoli Directory Server Version 6.2 or above

There are several functions that have not been part of the evaluation:

- Message protection policies
- Policy Information Points (PIP)
- Apart from web services, policies can also be applied to protect other types of resources (e.g. Databases). However, this has not been part of the evaluation.

The TOE is a distributed software. Its components are divided on three server machines as shown in figure 1 “Typical TSPM Deployment Diagram” of the Security Target [6].

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

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

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

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

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

9.2 Results of cryptographic assessment

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

10 Obligations and Notes for the Usage of the TOE

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

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

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

11 Security Target

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

12 Definitions

12.1 Acronyms

AIS	Application Notes and Interpretations of the Scheme
APAR	Authorized Problem Analysis Report
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
J2EE	Java 2 Enterprise Edition
LDAP	Lightweight Directory Access Protocol
PAP	Policy Administration Point
PDP	Policy Decision Point
PDT	Policy Distribution Target
PEP	Policy Enforcement Point
PIP	Policy Information Points
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
RTSS	Runtime Security Services

SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TCR	Tivoli Common Reporting
TIP	Tivoli Integrated Portal
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSPM	Tivoli Security Policy Manager
WAS	WebSphere Application Server
XACML	eXtensible Access Control Markup Language

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

13 Bibliography

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

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[9].

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

[6] Security Target BSI-DSZ-CC-0839-2013, Version 1.24, 2013-10-31, Tivoli Security Policy Manager Version 7.1 Security Target, IBM Corporation

[7] Evaluation Technical Report, Version 3, 2013-11-05, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

13.1 Guidance documentation

[8] Security Policy Manager Version 7.1.0.4 Common Criteria Guide, SC27-5627-00

[9] Security Policy Manager Version 7.1 Administration Guide, SC23-9476-01

[10] Security Policy Manager Version 7.1 Configuration Guide, GC27-2713-00

[11] Security Policy Manager Version 7.1 Installation Guide, GC27-2712-00

[12] Security Policy Manager Version 7.1 Troubleshooting Guide, GC27-2711-00

[13] Security Policy Manager Version 7.1 Error Message Reference, GC23-9477-01

[14] TSPM Online Fix Pack 4 Guidance,
http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=
%2Fcom.ibm.tspm.doc_7.1%2Fwelcome.html

[9] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

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

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

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

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

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

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

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

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

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

The following table shows the assurance class decomposition.

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

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

Assurance class decomposition

Evaluation assurance levels (chapter 8)

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

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

Evaluation assurance level (EAL) overview (chapter 8.1)

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

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

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

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

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

Table 1: Evaluation assurance level summary”

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

“Objectives

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

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

“Objectives

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

Class AVA: Vulnerability assessment (chapter 16)

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

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

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

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

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.