Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0636-2012

for

IBM Tivoli Access Manager for e-Business version 6.1.1 FP4 with IBM Tivoli Federated Identity Manager version 6.2.1 FP2

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-0636-2012

Access Manager

IBM Tivoli Access Manager for e-business version 6.1.1 FP4 with
IBM Tivoli Federated Identity Manager version 6.2.1 FP2

from	IBM Corporation
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 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, 22 June 2012
For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

Bernd Kowalsk
Head of Department

L.S.

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

[1] Act 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 IBM Tivoli Access Manager for e-Business version 6.1.1 FP4 with IBM Tivoli Federated Identity Manager version 6.2.1 FP2 has undergone the certification procedure at BSI.

The evaluation of the product IBM Tivoli Access Manager for e-Business version 6.1.1 FP4 with IBM Tivoli Federated Identity Manager version 6.2.1 FP2 was conducted by atsec information security GmbH. The evaluation was completed on 30 May 2012. 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.

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

[6] Information Technology Security Evaluation Facility

- 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 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.

5 Publication

The product IBM Tivoli Access Manager for e-Business version 6.1.1 FP4 with IBM Tivoli Federated Identity Manager version 6.2.1 FP2 has been included in the BSI list of the 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

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 Tivoli Access Manager for e-business 6.1.1 FP4 with Tivoli Federated Identity Manager 6.2.1 FP2 with the following elements:

- Tivoli Access Manager for e-business 6.1.1 FP4 (TAMeb)
- Tivoli Federated Identity Manager 6.2.1 FP2 (TFIM)

The TAMeb portion of the TOE follows the access control framework defined by the ISO 10181-3 standard [12] and the Authorization API (aznAPI) [13]. TFIM is an identity mapping application used to map identities between disparate organizations allowing users to single sign on to multiple organizations. The TAMeb portion of the TOE contains a component called WebSEAL. WebSEAL acts as a reverse web proxy by receiving HTTP/HTTPS requests from a web browser and, when allowing access, it forwards the request to the junctioned back-end web application servers (a.k.a. target systems), and finally delivers the server responses back to the user.

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

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functions	Addressed issue
Audit	The TOE provides auditing of authentication and authorization attempts, administrative actions, and single sign-on operations.
Authentication	The TOE provides: ● Authentication services via passwords and certificates with support by the TOE operational environment. ● Single sign-on via SAML 1.1 with support of the TOE operational environment.
Authorization	The TOE provides authorization services using a standard authorization API providing authorization decisions based on: ● Fine-grained access control lists that control access to protected resources using various permission types dependent on the performed action, simplified by a hierarchical view of the protected web and management resources. ● Protected object policies that allow access based on conditions like time and day of access, the request origin in the network, and the used authentication mechanism and communication type.
Management	The TOE provides management of authentication mechanisms and access control.

Table 1: TOE Security Functionalities

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

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

This certification covers the following configurations of the TOE: Tivoli Access Manager for e-business 6.1.1 Fix Pack 4 and Tivoli Federated Identity Manager 6.2.1 Fix Pack 2. For details refer to chapter 8.

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

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

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

IBM Tivoli Access Manager for e-business version 6.1.1 FP4 with IBM Tivoli Federated Identity Manager version 6.2.1 FP2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
Tivoli Access Manager for e-business 6.1.1 FP4				
1	SW	Tivoli Access Manager for e-business	6.1.1	secure download
2	SW (fix pack)	6.1.1-TIV-TAM-FP0004-'platform'	4	secure download
3	DOC	TAMeb User/Administrator Guidance [10]		secure download
		Installation Guide	GC23-6502-01	
		Base Administration Guide	SC23-6504-01	
		WebSEAL Administration Guide	SC23-6505-01	
		Command Reference	SC23-6512-01	
		Auditing Guide	SC23-6511-01	
		Error Message Reference	GI11-8157-01	
Tivoli Federated Identity Manager 6.2.1 FP2				
4	SW	Tivoli Federated Identity Manager	6.2.1	secure download
5	SW (fix pack)	6.2.1-TIV-TFIM-FP0002	2	secure download
6	DOC	TFIM User/Administrator Guidance [11]		secure download
		Installation Guide	GC27-2718-00	
		Configuration Guide	GC27-2719-00	
		Administration Guide	SC23-6191-01	

No	Type	Identifier	Release	Form of Delivery
		Auditing Guide	GC32-2287-03	
		Error Message Reference	GGC32-2289-03	
IBM Tivoli Access Manager for e-business version 6.1.1 FP4 with IBM Tivoli Federated Identity Manager version 6.2.1 FP2				
7	DOC	Common Criteria Guide [9]	SC23-6138-01	secure download

Table 2: Deliverables of the TOE

All TOE elements are delivered via a secure download (HTTPS) from the IBM web page. This requires the use of the Download Director which is an applet provided on the IBM web page once a TOE element has been chosen for download.

- The TOE base packages (TAMeb 6.1.1 and TFIM 6.2.1) can be obtained from Passport Advantage (http://www.ibm.com/software/passportadvantage/) for which an IBM account is required.
- The Fix Packs can be obtained from IBM Fix Central (http://www.ibm.com/support/fixcentral) for which an IBM account is required.
- The guidance can be obtained from the IBM support page (http://www.ibm.com/support). Specifically the Common Criteria Guide can be found by searching for SC23-6138-01, and should then be downloaded securely choosing the Download Director option. This Common Criteria Guide contains more details on the secure delivery for the TOE components and fix packs mentioned above.

The Common Criteria Guide [9] refers to the versions of the TOE and the fix packs. It further describes the procedure for downloading the TOE. On these pages, the user can identify the TOE with the help of these version numbers.

Upon installation, the TOE versions can also be identified through using version utilities as follows:

- For TAMeb and WebSEAL: command line utility pdversion
- For TFIM: viewing the configured TFIM runtime environment in the WebSphere administration console.

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:

- Audit
- Authentication
- Authorization
- Management

For more information on these issues, see Security Target [6], chapter 1.4.12.

4 Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of 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 has to be ensured that protected resources cannot be accessed in a way that bypasses the TOE and that all internal and external access attempts to protected resources have to be channeled through the TOE.
- Users have to administer and protect private keys of their client system used for authentication and key exchange with the TOE in a secure way.
- Users and administrators have to protect their passwords used for authentication to the TOE.
- The machines running the TOE software need to be protected against unauthorized physical access and modification.
- Any machine used to run all or a part of the TOE software are assumed to be used solely for this purpose.
- The operating system of the machines running the TOE is assumed to be configured and maintained by trained and trustworthy personnel.
- The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation. They will perform administration activities from a secure environment using terminals and/or workstations they trust via secured connections to the Policy Server.
- The Directory Server used by the TOE provides protection mechanism against unauthorized access to TSF data stored in the directory.
- The operational environment protects credentials against unauthorized access.
- The operational environment components that implement TLS used by the TOE and the operational environment components generating and interpreting SAML responses implement their security protocols and cryptographic functions correctly.
- The TOE components reside within a protected network.
- The TFIM audit mechanism will only be configured during TFIM installation or when TFIM is in an offline mode of operation.
- Communication of TOE external entities with the TOE as well as communication between physically distributed parts of the TOE are secured using TLS.
- Only administrators authorized for access to defined management resources of the TOE may access those resources after they have been successfully authenticated.
- Only those users who have been authorized to access web resources protected by the TOE may access those resources after they have been successfully authenticated.
- Passwords for both administrative accounts and user accounts should have sufficient strength as commensurate with the importance of the information protected by the accounts.

Details can be found in the Security Target [6], chapter 3.2 and 3.3.

5 Architectural Information

The TOE consists of the Tivoli Access Manager for e-business (TAMeb) and the Tivoli Federated Identity Manager (TFIM).

TAMeb is a complete authorization solution for corporate web, client/server, Tivoli Access Manager applications, and legacy (pre-existing) applications. TAMeb allows an organization to securely control user access to protected information and resources located within the organizations infrastructure. TAMeb itself is comprised of the Policy Server and WebSEAL. The Policy Server maintains an authorization database that is kept in sync with WebSEAL. User requests are handled by WebSEAL on the basis of this database information controlling access to requested remote web resources.

WebSEAL users and administrators are defined in an LDAP server which is queried by the Policy Server and WebSEAL upon user authentication. TAMeb therefore allows controlled access to its registered web resources and the architectural view would be as follows:

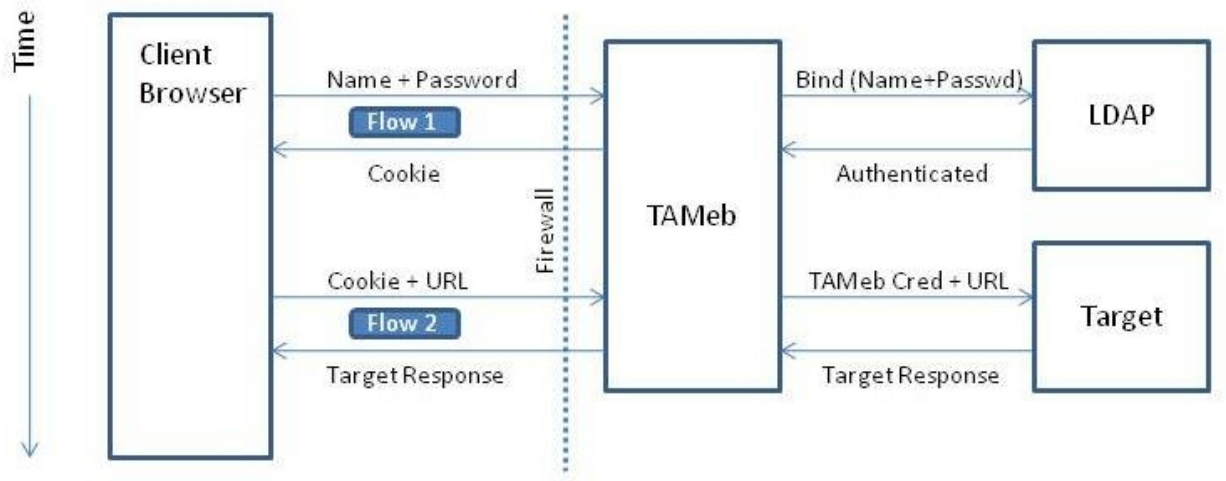

Figure 1: Data flow without SSO

Tivoli Federated Identity Manager (TFIM) aids in mapping identities between disparate organizations (each organization has an PolicyServer/WebSEAL/TFIM setup) allowing organizations to maintain their current identification mechanisms and control which identities have cross organizational access. TFIM is used as a federated single sign-on (F-SSO) solution allowing users to enter their authentication data once and be granted access to several systems across organizations. In the evaluated configuration, TFIM supports the Security Assertion Markup Language (SAML) 1.1 Browser/POST Profile for exchanging user identities between other federated identity managers.

For the federated single sign-on, the TAMeb and TFIM component work in concert to generate a signed token that can be verified by the PolicyServer/WebSEAL/TFIM components at the partner organization to grant access to their resources. The identity is only once determined at the identity provider and reused for all further requests on the service provider side:

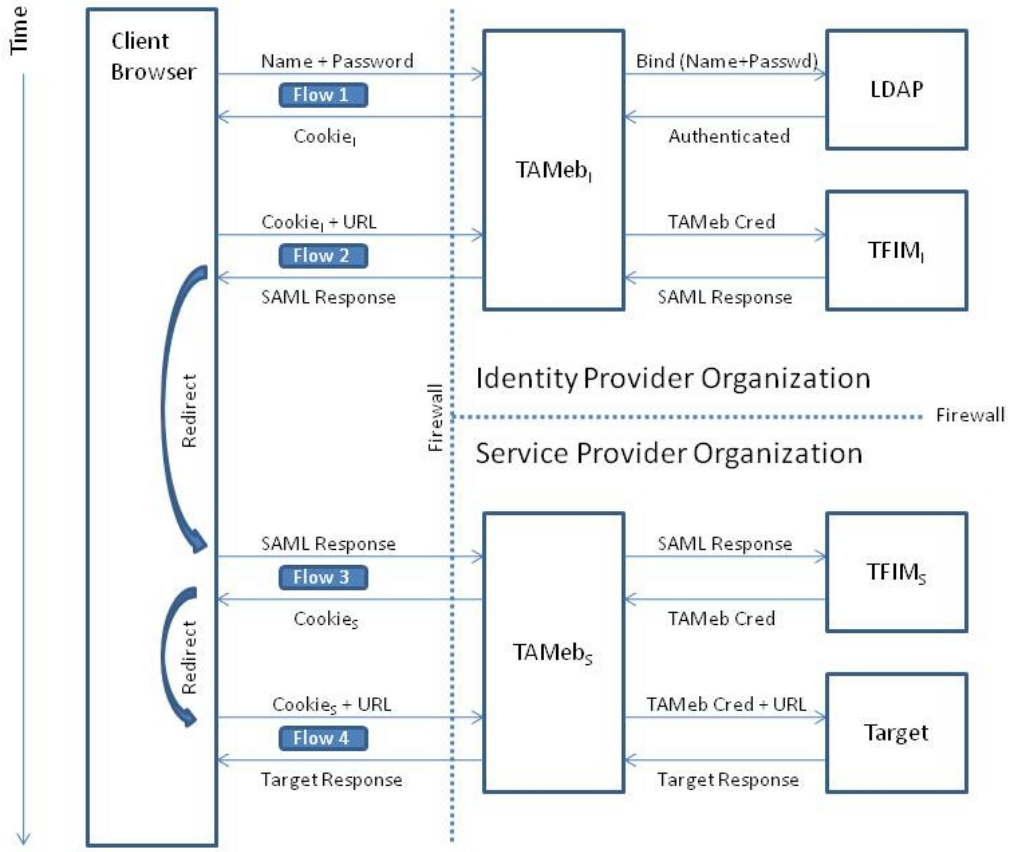

Figure 2: Data flow with SSO

The logical boundary of the TOE is as follows: The TFIM Runtime, TFIM Management Service, Policy Server, the Resource Manager/Authorization Evaluator, the Master Authorization Policy database as well as the Replica Authorization Policy database are part of the TOE. The WebSphere Application Server (for TFIM), WAS Deployment Manager, Directory Server, the Client system as well as the web application servers are all part of the operational 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

The developer and evaluator testing was performed according to the evaluated configuration with some minor deviations for the evaluator tests not relevant for the test results, i.e. Policy Server and WebSEAL were installed on one test machine, simple passwords were used, HTTP/s was disabled for chosen tests and authorization rules were

not disabled. All platforms supported by the evaluated configuration have been tested by the developer, while the evaluator performed the independent evaluator tests on the Windows platform.

7.1 Developer Testing

The developer test cases comprise of 21 manual test files that define the major test cases. The amount of testing work done for each test case differed between a few instructions for testing one Security Function to up to 19 pages covering several related Security Functions. The tests have been specifically designed to meet the CC-requirements.

TOE Test Configuration

All TOE parts (WebSEAL, Policy server, TFIM) were installed on different machines. The evaluated configuration was performed according to the ST [6] and the CC Guide [9] that details the evaluated configuration. The developer set up three configurations, one for the Identity Provider side and one for the Server Provider side, and another setup was made where only WebSEAL/Policy Server tests were performed which do not require TFIM.

Testing Approach

The test cases have been designed to cover all SFRs. Based on a TSFI/SFR mapping which shows test coverage of the TSFIs, the developer originally included the tested SFRs in the test case documentation to determine that the Security Functional Requirements are covered. They were removed in the final test case version.

The developer used a cross-coverage approach for testing on all supported platforms without configuring all possible test permutations for the different TOE components. The C-based and therefore generally more platform-dependent parts Policy Server and WebSEAL have been tested on all platforms except for the similar Linux distributions where the tests have been split up between these two supported platforms (SLES and RHEL). The generally less operating system platform dependent TFIM (it is a Java application running inside the WebSphere application server) has been tested on two major platform types (Windows-based and Unix-based).

OS / TOE component	TAM (Policy Server)	WebSEAL	TFIM
Windows Server 2008 (32bit)	+	+	+
Red Hat Enterprise Linux 5 (32bit)	+		+
SUSE Linux Enterprise Server 10 (32bit)		+	
AIX 6.1 (64bit)	+	+	

The developer test configuration included the following platform combinations:

- Without TFIM:
  - TAM: AIX 6.1
  - WebSEAL: AIX 6.1
- TFIM Identity Provider:
  - TFIM: Windows Server 2008
  - TAM: Windows Server 2008
  - WebSEAL: Windows Server 2008

- TFIM Service Provider:
  - TFIM: RHEL 5
  - TAM: RHEL5
  - WebSEAL: SLES 10 SP1

The developer used a TSFI test mapping to ensure that all TSFIs were tested, and that all SFRs were tested. The Security Function test was performed down to individual SFR statements.

Conclusion

All developer tests were run successfully. The tests results demonstrate that no discrepancy between the TOE behavior and the TOE specification has been found.

7.2 Evaluator Independent Testing

The evaluator devised 19 independent functional tests. Also, a small subset of the developer tests were rerun together with the developer on their test machines via a remote web meeting.

TOE Test Configuration

The evaluator installed the different components of the TOE on two machines in each domain resulting in four installations. The evaluator chose one of the supported operating system platform types (Windows Server 2008) for all four server machines (running as virtual machines) running on one physical test machine. In addition, another physical machine is hosting two LDAP server instances and a target web server that hosts the remote resources that are protected by the TOE.

The evaluated configuration according to the CC Guide [9] has been applied to TOE platforms only omitting a few configuration settings that were not relevant for the test results.

Testing Approach

Most of the tests were standard tests using the external visible interfaces as described in the user guidance. For the following instances the evaluator used additional means to better test a specific TOE behavior:

- An external library used by the TOE has been tested directly using a documented API of that library, without going through the external TOE interfaces, to have better control over the function input.
- Removal/modifications of key store files that are used internally by the TOE, followed by a rerun of the single sign-on tests.

Most of the tests are manual tests with the exception of two cases where java test scripts have been created by the evaluator. The evaluator also modified some TOE configuration state information (not an external interface), e.g., key stores to verify that the dependent Security Functions still behave as expected.

Tested Interfaces

The evaluator focused on the three main TSFIs of the TOE:

- WebSEAL client interface: The main attack surface of the TOE.

- TFIM runtime interface: it includes the SAML protocol messages which are not visible to 3rd-parties as they are wrapped inside TLS.
- pdadmin console: The main TOE management interface.

With these interfaces which the evaluator considered the main TSFIs, the evaluator also covered most TSF areas including I&A, Access Control and Security Management. The Auditing and SSO I&A Security Functions have also been tested via Live Web Meeting including the execution of modified versions of the developer tests.

Conclusion

All independent tests were run successfully. The TOE security functionality and TSFI behave as specified in the Security Functional Requirements.

7.3 Evaluator Penetration Testing

TOE Test Configuration

The same test configuration as for the independent tests has been used.

Testing Approach

The tested TSFIs were:

- WebSEAL client interface: The main attack surface of the TOE and subject to the majority of the tests.
- TFIM runtime interface: It includes the SAML protocol messages which are not visible to 3rd-parties as they are wrapped inside TLS.

The test set consisted of eight test cases including some variations. Most tests were manual tests, enhanced by a general vulnerability scan.

Conclusion

All tests were run successfully. None of the tests revealed any exploitable vulnerabilities.

8 Evaluated Configuration

This certification covers the following configurations of the TOE: Tivoli Access Manager for e-business 6.1.1 Fix Pack 4 and Tivoli Federated Identity Manager 6.2.1 Fix Pack 2.

The operational environment includes the following software products:

- IBM WebSphere Application Server (WAS) version 7.0.0.11 (includes Java)
- IBM WebSphere Application Server Deployment Manager version 7.0.0.11
- IBM HTTP Server (IHS) 6.1 WAS Plug-in
- IBM GSKit (Global Security Kit), version 7.0.4.33
- Directory Server (LDAP), version 6.1

The operational environment consists of the following hardware platforms and operating systems:

- AIX 6.1 (64-bit)
- Windows Server 2008 Enterprise (32-bit)

- SUSE Linux Enterprise Server 10 SP1 on IBM xSeries (32-bit)
- Red Hat Enterprise Linux Version 5 on IBM xSeries (32-bit)

Further information on the evaluated configuration can be found in the Security Target [6], chapter 1.4.10.

9 Results of the Evaluation

9.1 CC specific results

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

The Evaluation Methodology CEM [2] was used.

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.3 augmented for this TOE evaluation.

The evaluation has confirmed:

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

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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 and Operational Security Policies 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
aznAPI	Technical Standard Authorization (azn) API
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
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SLES	SUSE Linux Enterprise Server
SSO	Single Sign-On
ST	Security Target
TAMeb	Tivoli Access Manager for e-business
TFIM	Tivoli Federated Identity Manager
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

TSFI TSF Interface

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 - An 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, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

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

[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), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0636-2012, Version 1.30, 16th May 2012, Tivoli Access Manager for e-business 6.1.1 FP4 with Tivoli Federated Identity 6.2.1 FP2 Security Target

[7] Evaluation Technical Report, Version 3, 25th May 2012, Final Evaluation Technical Report, atsec information security GmbH (confidential document)

[8] Configuration lists for the TOE (confidential documents)

[CIL-FLR] Lists the security flaw configuration items, 19th November 2010, TAMeb 6.1.1/TFIM 6.2.1 Security Flaw Remediation Report

[CIL-SC1] Lists the source code file names/versions for the TAM Base runtime 6.1.1 FixPack 4 components, 30th November 2011, Source code file names/versions for the TAM Base runtime 6.1.1 FixPack 4 components

[CIL-SC2] Lists the source code file names/versions for the TAMeb WebSeal server 6.1.1 FixPack 4 components, 30th November 2011, Source code file names/versions for the TAMeb WebSeal server 6.1.1 FixPack 4 components

[CIL-SC3] Lists the source code file names/versions for the TAMeb WebSeal server runtime 6.1.1 FixPack 4 components, 30th November 2011, Source code file names/versions for the TAMeb WebSeal server runtime 6.1.1 FixPack 4 components

[CIL-SC4] Lists the source code file names/versions for the TFIM 6.2.1 FixPack2 components, 30th November 2011, Source code file names/versions for the TFIM 6.2.1 FixPack 2components

[CIL-SC5] Lists the source code file names/versions for utility libraries that are used with the TAMeb 6.1.1 FixPack 4 product, 30th November 2011, Source code file names/versions for utility libraries that are used withthe TAMeb 6.1.1 FixPack 4 product

[CIL-GD-TAM] Lists the GSA configuration items (TAMeb), 23rd November 2010, TAMeb 6.1.1 IDD Source files listing

[CIL-GD-TFIM] Lists the CMVC configuration items (TFIM and CC Guide), 8th February 2012, TFIM 6.2.1 IDD files source listing

[8] specifically

- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema

[CIL-TESTS] Lists test plan, ST to RQM mapping, test cases, and test results, 15th November 2011, Test Cases and Results Configuration List

[CIL-CCEV] Lists the remaining evidence configuration items for the CC evaluation, 22nd February 2012, Common Criteria Evaluation evidence configuration list

[9] Guidance documentation for the TOE, SC23-6138-01, 19th April 2012, Tivoli Access Manager for e-business 6.1.1 and Federated Identity Manager 6.2.1 Common Criteria Guide

[10] Additional guidance documentation for TAMeb

[TAMINST] Installation Guide, GC23-6502-01, 17th November 2010, Tivoli Access Manager for e-business Version 6.1.1 Installation Guide

[TAMADM] Base Administration Guide, SC23-6504-01, 17th November 2010, Tivoli Access Manager for e-business Version 6.1.1 Administration Guide

[WSADM] WebSEAL Administration Guide, SC23-6505-01, 17th November 2010, Tivoli Access Manager for e-business Version 6.1.1 WebSEAL Administration Guide

[CMD] Command Reference, SC23-6512-01, 8th December 2010, Tivoli Access Manager for e-business Version 6.1.1 Command Reference

[TAMAUD] Auditing Guide, SC23-6511-01, 26th October 2010, Tivoli Access Manager for e-business 6.1.1 Auditing Guide

[TAMERR] Error Message Reference, GI11-8157-01, 18th November 2010, Tivoli Access Manager Version 6.1.1 Error Message Reference

[11] Additional guidance documentation for TFIM

[TFIMINST] Installation Guide, GC27-2718-00, 27th September 2011, Tivoli Federated Identity Manager Version 6.2.1 - Installation Guide

[TFIMCFG] Configuration Guide, GC27-2719-00, 8th December 2010, Tivoli Federated Identity Manager Version 6.2.1 Configuration Guide

[TFIMADM] Administration Guide, SC23-6191-01, 17th November 2010, Tivoli Federated Identity Manager Version 6.2.1 Administration Guide

[TFIMAUD] Auditing Guide, GC32-2287-03, 26th October 2010, Tivoli Federated Identity Manager Version 6.2.1 Auditing Guide

[TFIMERR] Error Message Reference, GC32-2289-03, 18th November 2010, Tivoli Federated Identity Manager Version 6.2.1 Error Message Reference

[12] ISO 10181-3, 1996, Information Technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework

[13] aznAPI, January 2000, Open Group Technical Standard: Authorization (AZN) API, The Open Group

C Excerpts from the Criteria

CC Part1:

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.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0636-2012

Evaluation results regarding development and production environment

The IT product IBM Tivoli Access Manager for e-Business version 6.1.1 FP4 with IBM Tivoli Federated Identity Manager version 6.2.1 FP2 (Target of Evaluation, TOE) 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.

As a result of the TOE certification, dated 22 June 2012, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_FLR.3, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

a) IBM Austin, 11501 Burnet Rd, Austin, TX 78758 (Design and Development)

b) IBM Research Triangle Park, 3901 S Miami Blvd., Durham, NC 27703 (Configuration Management Server)

c) IBM Gold Coast, L11 and L7 Seabank 12-14 Marine Parade Southport, QLD 4215 (Design and Development)

d) IBM Singapore Development Lab, 7 Changi Business Park, Central 1, Singapore, 486072 (Development of TOE Guidance, Testing)

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.