Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0683-2014

for

IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2

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-0683-2014

Access Control System

IBM Security Access Manager for Enterprise Single Sign-On
Version 8.2

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

SOGIS
Recognition Agreement

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. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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.

Common Criteria
Recognition Arrangement

Bonn, 5 December 2014

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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:

- Act on the Federal Office for Information Security[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 ISO/IEC 17065 standard
- BSI certification: Technical information on the IT security certification, Procedural Description (BSI 7138) [3]
- BSI certification: Requirements regarding the Evaluation Facility (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- 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 EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined.

---

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

It includes assurance levels beyond EAL 4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2 International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

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.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. for all assurance components selected.

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 Security Access Manager for Enterprise Single Sign-On, Version 8.2 has undergone the certification procedure at BSI.

The evaluation of the product IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2 was conducted by atsec information security GmbH. The evaluation was

completed on 31 October 2014. 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,
- 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 IBM Security Access Manager for Enterprise Single Sign-On, Version 8.2 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.

---

6 Information Technology Security Evaluation Facility

7 IBM Corporation
11501 Burnet Road
Austin
Texas

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 Security Access Manager for Enterprise Single Sign-On Version 8.2 with IMS Server Interim Fix 4 and AccessAgent Fix Pack 22. It is an enterprise single-sign-on product for Microsoft Windows-based systems. The TOE automatically, driven by rules, enters user credentials into credential-requesting applications on behalf of the user once the user has successfully authenticated to the TOE. The TOE further provides functions to audit user actions, protect the user's data and manage these TOE security functions.

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

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 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 Functionality:

TOE Security Functionality	Addressed issue
Audit	Various components of the product generate audit events which are stored in the IMS Server database. All user application access logs are collated into the IMS Server's audit log database. Each log record contains info related to time and location from which a user accesses a certain application.
Identification and Authentication	The TOE supports an identification mechanism and an authentication mechanism. The TOE maintains its own user repository and performs user authentication against various forms of authentication credentials stored in this repository (stored in the IMS Server database). The user's ISAM E-SSO Password is created when the account is first created (when the user first sign's up).
User Data Protection	The TOE supports a user data protection mechanism. The TOE stores each user's credential data in a Wallet; one Wallet per-user. A Wallet provides confidentiality and integrity protection of the user credential data through the use of cryptographic operations. All cryptographic operations are performed by the Operational Environment.
Security management	The TOE supports security function management mechanisms. Role-based access control is used to protect access to operations in the AccessAdmin and AccessAssistant applications.

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], chapter 3.1 - 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 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 Security Access Manager for Enterprise Single Sign-On, Version 8.2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	IBM Security Access Manager for Enterprise Single Sign on Suite (32bit)	8.2.0, Part Number CRH6SML	DL
2	SW	IBM Security Access Manager for Enterprise Single Sign on Suite (64bit)	8.2.0, Part Number CRH6TML	DL
3	SW	IMS Server Interim Fix 04	8.2.0 (8.2.0-ISSSAMESSOIMSIF0004.zip)	DL
4	SW	Access Agent Fixpack 22 (32bit)	8.2.0 (8.2.0-ISSSAMESSOAAFP0022_32.msp)	DL
5	SW	Access Agent Fixpack 22 (64bit)	8.2.0 (8.2.0-ISSSAMESSOAAFP0022_64.msp)	DL
6	DOC	IBM Security Access Manager for Enterprise Single Sign-On Common Criteria Guide	8.2.0 (SC27-4365-00)	DL
7	DOC	IBM Security Access Manager for Enterprise Single Sign-on Quick Start Guide	8.2.0 (GI11-8732-03)	DL
8	DOC	IBM Security Access Manager for Enterprise Single Sign-on Installation Guide	8.2.0 (GI11-9309-01)	DL
9	DOC	IBM Security Access Manager for Enterprise Single Sign-on Configuration Guide	8.2.0 (GC23-9692-01)	DL
10	DOC	IBM Security Access Manager for Enterprise Single Sign-on Deployment Guide	8.2.0 (SC23-9952-03)	DL
11	DOC	IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide	8.2.0 (SC23-9951-03)	DL

No	Type	Identifier	Release	Form of Delivery
12	DOC	IBM Security Access Manager for Enterprise Single Sign-on User Guide	8.2.0 (SC23-9950-03)	DL
13	DOC	IBM Security Access Manager for Enterprise Single Sign-on Help Desk Guide	8.2.0 (SC23-9953-03)	DL
14	DOC	IBM Security Access Manager for Enterprise Single Sign-on Troubleshooting and Support Guide	8.2.0 (GC23-9693-01)	DL
15	DOC	IBM Security Access Manager for Enterprise Single Sign-on AccessStudio Guide	8.2.0 (SC23-9956-03)	DL
16	DOC	IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide	8.2.0 (SC23-9694-01)	DL
17	DOC	IBM Security Access Manager for Enterprise Single Sign-on Provisioning Integration Guide	8.2.0 (SC23-9957-03)	DL
18	DOC	IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide	8.2.0 (SC14-7646-00)	DL
19	DOC	IBM Security Access Manager for Enterprise Single Sign-on Context Management Integration Guide	8.2.0 (SC23-9954-03)	DL
20	DOC	IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide	8.2.0 (SC14-7626-00)	DL
21	DOC	IBM Security Access Manager for Enterprise Single Sign-On Lightweight AccessAgent mode on Terminal Server SDK Guide	8.2.0 (SC14-7657-00)	DL
22	DOC	IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide	8.2.0 (GC14-7624-00)	DL

Table 2: Deliverables of the TOE

The TOE is electronically downloaded using 2 steps:

1. The base version of the TOE is to be downloaded from passport advantage.
2. The TOE Fixpacks as well as the documentation is electronically downloaded from the IBM support site.

The downloads are to be carried using the secure Download Director protocol.

The TOE can be identified by the user by its version numbers. The Access Agent version number is: 8.2.0.3458. The IMS Version number is: 8.2.0.696

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:

- **Access Profiles:** The TOE only releases a subset of the credential information stored in a user's Wallet to the target application the user intends to identify and authenticate to based on Access Profiles.

- **Audit:** The TOE shall offer an audit mechanism that can be used to hold users of each role accountable for security-relevant actions performed with the TSF.
- **Authentication:** The TOE must ensure that only authorized users gain access to the TOE and its resources.
- **Manage:** The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms and must ensure that only authorized users are able to access such functionality.
- **Role:** The TOE must assign a role to each user after successful identification and authentication to the management facility. This role limits the management actions the user is allowed to perform.
- **Password Quality:** When in GINA mode with Active Directory password synchronization disabled, the TOE must ensure that the quality of the ISAM E-SSO Password protecting the Common Symmetric Key (CSK) must possess the strength to prevent credential guessing from threat agents.
- **Wallet Access:** The TOE must ensure that users can only access the contents of the Wallet assigned to them.

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:

- Cryptographic operations
- Competent individuals
- Password quality
- Physical protection
- Runtime environment
- Time source
- Users

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

5 Architectural Information

The TOE consists of multiple components executing in a distributed environment and communicating using the network. Figure 1 in the Security Target [6] depicts the different components forming the product. Each of the green shaded components are described in the subsequent sections in the Security Target [6], chapter 1.5.2. These green shaded components together form the TOE.

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

The developer used 24 manual test cases where each test case may contain up to 100 sub tests (each test testing a specific aspect of a functionality).

Two test scripts are used that automatically test several functions related to wallet and role management. The developer test evidence comprises many more tests cases but the majority of them is not relevant for the evaluated functions.

7.1.1 Test Configuration

The developer tested all supported agent and IMS server platforms:

- AccessAgent on Windows XP/7 on 32bit and 64 bit (it includes GSKit which is part of the TOE environment)
- IMS server on Windows Server 2008 32bit and 64bit
- WebSphere 7 (which includes Java) for databases, IBM DB2, Microsoft SQL Server, and Oracle Database has been tested

Other settings relevant for the evaluated configuration (e.g. password strength or enable/disabling certain functions) have been only used when it is needed for the tests.

7.1.2 Test approach

The manual developer tests were designed to use the GUI (Access Agent or IMS server web interfaces). The manual tests consists of several test plan documents where one document refers to the regression testing. The regression testing is a large collection of tests that have been collected over time for each new version of the product. This ensures that old functions still work on the latest release version.

The automated tests use the IMS API which is an internal TOE interface to the IMS server.

7.1.3 Testing Results

The developer testing was performed successfully with no exceptions by the developer on all supported platforms.

7.2 Evaluator Testing Effort

The evaluator chose 28 developer tests for independent testing and created 7 new test cases.

7.2.1 Test Approach and Depth

The evaluator witnessed parts developer tests via a web conference, where a subset (9 developer tests) of the developer tests were executed based on the evaluator's choice.

18 other developer tests and all but one evaluator test have been executed on in the ITSEF lab where the TOE has been installed. The evaluator test which involves the use of the AccessStudio for access profiles application was performed on the developer test systems.

The evaluators choice of the developer tests was to test all security functions (apart from the auditing) and to also see all different types of supported platforms working. Specifically, the following areas are covered by the independent testing of developer tests:

- releasing credentials to web applications and non-web applications as the core functionality of the single-sign on operations
- authentication of AccessAgent users and IMS administrators
- policy management by help desk and administrative user roles
- password management by users

For the evaluator tests, the focus lay on:

- audit generation and review, especially testing the interaction between the AccessAgent and the IMS server so that audit events get exchanged
- AccessAgent authentication in case the respective AD user account gets changed (e.g. disabled) or client installation is not part of the AD domain
- creation and application of access profiles (the access profile that was created as part of this test was used as input to the penetration testing when attempting to obtain user credentials by forging applications)

All subsystems have been tested: while the tests of the user authentication applied to the AccessAgent, all management and admin authentication tests used the AccessAdmin and AccessAssistant subsystems. The IMS runtime was tested indirectly by using the AccessAgent because the agent uses the IMS server interface to communicate with the server. The configuration utilities were tested too as part of the access profile upload and TOE configuration steps.

7.2.2 Test Configuration

The evaluator test configuration was the following:

- two AccessAgent (FixPack 22) client machines with WinXP 32-bit as underlying platform
- IMS (Interim Fix 4) server installation with Windows Server 2008 32-bit as underlying platform
- Active Directory as User Registry
- Applied configuration according to the evaluate configuration in the guidance as necessary for the testing
- IBM DB2 9.7

The developer test setup consisted of a broader number of platforms (covering all platforms that are defined for the evaluated configuration):

- AccessAgent: WinXP 32/64 bit, Windows 7 32/64 bit
- IMS Server: Windows Server 2008 32/64 bit

7.2.3 Test Results

All tests have been performed successfully with the actual results matching the expected results.

7.3 Evaluator Penetration Testing

The evaluator used the CVE for finding publicly documented vulnerabilities. None of the found entries required independent testing.

The test effort based on all the developer evidence lead to the test of 14 potential vulnerabilities, where some vulnerabilities might apply to a number of different functions. Therefore, several tests where subdivided into testing the vulnerability aspect on several functions.

The test approach was to generally aiming at authentication and authorization functions of the TOE, i.e., the IMS server that enforces these security functions. This has been performed through attempting to gain access to TOE interfaces that should not be externally accessible, or use functions with unexpected parameter values (e.g. the AccessAgent uses the IMS server login functions by always providing the correct domain identifier, which is not the case when crafting requests to the IMS server manually). Considering the type of the security functions that were attempted to violate, the testing can be divided into these effects:

Testing the usability of invisible/deprecated functions that may violate authentication TSF, as well as standard authentication functions with ill-formed parameters.

Testing the usability of invisible/deprecated functions that may violate authorization TSF, as well as standard authorization functions.

Implicit test of wallet integrity through manipulating wallet data and its effect on single sign for application. A brute-force attack was tested to verify whether the SFR for verification of secrets holds.

Other tests were not target against a specific security objective, but attempted to observe any suspicious behavior as a result of the ill-formed input data tests, which could then be further analyzed.

Another group of tests where used to spot any interface functions among the complex SOAP and WebSphere provided interfaces, that are available despite being hidden from the network view according to the FSP. Any unexpectedly available interface could be used to violate management function requirements.

7.3.1 Test configuration

The tests were performed on the TOE that was installed on one of the supported WebSphere Application Server 7.0 on a Microsoft Windows Server 2008 32-bit platform for the IMS server and a Microsoft Windows XP client installation. 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).

7.3.2 Results

The tests showed that a few more functions allow a password authentication but none of the penetration tests revealed an exploitable vulnerability.

8 Evaluated Configuration

This certification covers the following configuration of the TOE:

- The use of personal secrets must be disabled.
- Only the AccessAgent plugins provided with the TOE are allowed.
- Only the ISAM E-SSO Password authentication factor is allowed.
- Second factor authentication is disallowed.
- Self-service policies:
  - Self-service password reset must be disabled.
  - Self-service authorization code issuance must be disabled.
  - Self-service registration and bypass of 2nd factor must be disabled.
  - Self-service registering of additional secrets during sign-up must be disabled.
- The IMS Server's master secret must be protected to only allow the Administrator role access to it.
- One-Time Passwords (OTPs) must be disabled.
- Mobile ActiveCode (MAC) must be disabled.
- Roaming Desktops (i.e., the use of Microsoft Windows Terminal Server and Citrix Presentation Server) must be disabled.
- RADIUS authentication must be disabled.
- Windows Fast User Switching must be disabled on Windows 7 systems running AccessAgent.
- Private Desktop must be disabled on Windows XP systems running AccessAgent.
- Single sign-on to AccessAdmin when using Microsoft Internet Explorer must be disabled.
- The IMS Server/application must be the only application running in the WebSphere Application Server (WAS).
- The TOE's password synchronization option with Active Directory affects the security of the TOE. Specifically, enabling password synchronization with Active Directory will disable the TOE's ability to enforce password quality requirements.
- The feedback email settings in AccessAssistant and Web Workplace must not be enabled.

9 Results of the Evaluation

9.1 CC specific results

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

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 3 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 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 3 augmented by ALC_FLR.1

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 cryptographic mechanisms. 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 of 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

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

cPP Collaborative Protection Profile

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

12.2 Glossary

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

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

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 - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

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: Technical information on the IT security certification of products, protection profiles and sites (BSI 7138) and Requirements regarding the Evaluation Facility for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC (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-0683-2014, Version 1.19, 2014-03-05, IBM Security Access Manager for Enterprise Single Sign-On Version 8.2 with IMS Server Interim Fix 4 and AccessAgent Fix Pack 22 Security Target, IBM Corporation

[7] Evaluation Technical Report, Version 2, 2014-09-22, Final Evaluation Technical Report, atsec information security GmbH, (confidential document)

[8] CM Lists, file name: CM.LISTS.real-final-final-final.zip, Date: 2014-09-22

[9] Security Access Manager for Enterprise Single Sign-On: Configuration Guide, Version GC23-9692-01, Date: 2012-04-02

[8] specifically
- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 23, Version 3, Zusammentragen von Nachweisen der Entwickler (Collection of Developer Evidence)
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

This page is intentionally left blank.

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
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

Assurance Class	Assurance Components
	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.

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

“Objectives

EAL 1 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.

EAL 1 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.

EAL 1 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 EAL 1 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 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 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.

EAL 2 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 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 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 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 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. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 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 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 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 EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 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 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 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.

EAL 6 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 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
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”

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.”

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.