Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0248-2005

for

Java Intelligent Agent Componentware IV
Version 4.3.11

from

DAI- Labor
Technische Universität Berlin

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Telefon +49 228 9582-0, Infoline +49 228 9582-111, Telefax +49 228 9582-455

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0248-2005

Java Intelligent Agent Componentware IV Version 4.3.11

from

DAI- Labor Technische Universität Berlin

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 conformant**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL3**

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 19 January 2005

The President of the
Federal Office for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS-MRA

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

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.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.
Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

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

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

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

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

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

Contents

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

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

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

[4] Schedule of Cost for Official Procedures of the Federal Office for Information Security (BSI-Kostenverordnung, BSI-KostV) of 29th October 1992, Bundesgesetzblatt I p. 1838

[5] Proclamation of the Bundesministerium des Innern of 22nd September 2000 in the Bundesanzeiger p. 19445

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 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on March 3rd 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003.

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 Java Intelligent Agent Componentware IV, version 4.3.11 has undergone the certification procedure at BSI.

The evaluation of the product Java Intelligent Agent Componentware IV was conducted by T-Sytems GEI GmbH. The T-Sytems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The developer is DAI – Labor, Technische Universität Berlin.

The sponsor is Deutsche Telekom AG.

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 19 January 2005.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B -30.

The product Java Intelligent Agent Componentware IV, version 4.3.11 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline 0228/9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] DAI - Labor, Technische Universität Berlin, Salzufer 12, D-10587 Berlin

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.

Contents of the certification results

1 Executive Summary

The Target of Evaluation (TOE) is the Java Intelligent Agent Componentware IV, version 4.3.11 (also named JIAC IV in short) developed by DAI- Labor, Technische Universität Berlin.

The intended use of the TOE is to handle and protect services (e-business services) against obvious vulnerabilities during external communication to other (trustworthy) entities and on the local platform against attacks initiated from the network. The intended e-Business scenarios are e.g. services to get or offer proposals, trading transactions and communication for minor valued operations with a low requirement for protection.

The TOE is part of a software product running on a Java Virtual Machine (1.4.2_04) consisting of a multi- agent platform. It consists of agents responsible for security functional behaviour as well as offering and maintaining the infrastructure of the local platform by stationary management agents:

- Agent Management System (AMS): The AMS represents the basic services by integrating agents into the run-time environment. Every agent acting on the local platform is registered at the management system. Service registration data is gathered by the Directory Facilitator (DF), which is functionally a part of the AMS. This service is able to request and provide information from/to a public server (LDAP) that gathers information on services of Remote Platforms. To exchange data, the AMS establishes a SSL connection to build a trusted channel external entities. Internally the AMS communicates via the Agent Communication Channel (ACC) with locally resident agents.

- Security Agent (SA): The SA provides a list of valid Certificates and a Certificate Revocation List (CRL) generated and signed by the principal Certification Authority (CA). The SA checks the validity of signatures and the validity of Certificates and sends the result to the requesting agent. Certificates include identification data about trustworthy platforms (AMS agents) and their associated public key. The list of Certificates and the CRL can be updated in regular intervals specified by the platform Administrator. Therefore the SA is capable of managing trust relationships between the local AMS and the trustworthy Remote Platforms (RP), User Interfaces (UI) and the Certification Authority (CA).

- Alter Ego (AE): The AE represents the missing link between a graphical User Interface, that resides remotely on a Navigator platform, and the publicly accessible application services registered on the local platform. The AE is responsible for interpretation of the given human user commands.

Communication to external trustworthy entities such as CA, UI and RP is given by speech-acts. Further more mobile agent transfer is only allowed to and from trustworthy RP. Exchanged data between these entities is only accepted when it was send via trusted channel connections. Data exchange with the LDAP is given by plain text using the normal TCP/IP protocol.

Public distribution of the TOE is realised by Web page access. TOE is passed on over the links "JIAC IV" and then "Data and information about the certification release (authorized users only)" of the DAI-Labor's web pages for download. This link does specify a connection that can only be used by authorised users.

The TOE includes Software components only and provides the following security functionality:

- Selective Proof of Origin
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- Trusted path/ channel

The TOE Security Functional Requirements (SFR) used in the Security Target are Common Criteria Part 2 conform as shown in the following table:

SFR	Identifier
FCO_NRO.1	Selective Proof of Origin
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ETC.2	Export of user data with security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_ITC.2	Import of user data with security attributes
FDP_SDI.2	Stored data integrity monitoring and action
FDP_UIT.1	Data exchange integrity
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FIA_USB.1	User-subject binding
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.2	Secure security attributes

SFR	Identifier
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_FLS.1	Failure with preservation of secure state
FPT_TDC.1	Inter-TSF basic TSF data consistency
FTP_ITC.1	Inter-TSF trusted channel
FTP_TRP.1	Trusted path

table 1: TOE Security Functional Requirements

Note that some of the SFRs have been iterated in the Security Target. For details on the iteration and the required security functionality please refer to the Security Target [6], chapter 5.1.

The IT product JIAC IV was evaluated by T-Sytems GEI GmbH. The evaluation was completed on the 16th December 2004. T-Sytems GEI GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The developer is:

DAI- Labor
Technische Universität Berlin
Salzuferstraße 12
10587 Berlin

The sponsor of this evaluation is:

Deutsche Telekom AG
Zentralbereich Innovationsmanagement
Friedrich- Ebert- Allee 140
53113 Bonn

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C of this report).

The TOE meets the assurance requirements of assurance level EAL3.

[8] Information Technology Security Evaluation Facility

1.2 Functionality

The TOE JIAC IV provides the following Security Functions:

SSL connection

The TOE ensures the communication by using the SSL protocol according to SSL3.0/TLS1.0 with the cipher suite SSL_RSA_WITH_3DES_EDE_CBC_SHA and the following key length of RSA: 1024 or 2048bit, 3DES: 168bit, SHA: none.

The SSL protocol is based on valid certificates for both connection sides. SSL provides also mechanisms to detect data manipulation to protect against modification, deletion, insertion and replay.

Entity Identification and Authentication

The User Interface (UI), Remote platform (RP), Mobile agent and Certification Authority (CA) identify and authenticate themselves at the TOE by successful validation of their certificates.

Human Identification and Authentication

The TOE identifies and authenticates the human users directly after establishing the SSL connection to the User Interface. Therefore the user has to enter a login and a password. The TOE provides a mechanism to verify passwords with a minimal length of eight alphanumerical characters.

Error and Platform Management

In case of the detection of an error on which the management level cannot react with an appropriate error recovery the TOE switches into a secure state. Only the Administrator of the TOE is allowed to enable and disable its external communication. Further more the TOE restricts the ability to disable, enable or determine and modify the behaviour of functions executed by agents to the Administrator.

Access Control

The TOE accepts data such as user application data, identification and authentication data, speech-act data, mobile agent data, certificates and CRLs only when they are send over a SSL connection (“trusted SSL connect” set to “yes”) from a trustworthy interface to ensure the integrity and confidentiality of these data. On the other side the TOE only sends these over a SSL connection to a trustworthy interface.

Every user gets a role in dependence to its validated certificate so that they receive only data which are dedicated to them.

Furthermore the TOE maintains identification and authentication data that belongs to multiple human users so that the TOE can separate them. User application data, such as the result of a service agent acting on behalf of an identified and authenticated user, is always associated to a user by the service-ID.

The TOE is able to send and receive data about agents registered on platforms from or to a LDAP server. These data are transmitted in plain-text using a normal TCP/IP protocol ("trusted SSL connect" remains set to "no"). The TOE accepts no other plain-text than LDAP data that are agent registration information of platforms. The TOE is able to parse this data only if it addresses the platforms LDAP component (AMS-DF) correctly. On the other hand the TOE sends no other data in plain-text then LDAP data, which represents agent registration information about the local platform.

Management of security attributes

The TOE provides restrictive default values before any external connection will be established for the security attributes ("role" set to "none" and "trusted SSL connect" set to "no"). These default values cannot be overridden. The values of these attributes are set automatically in dependency on the successful establishment of a SSL connection based on a successful verification of the certificate provided by the CA. The CA does not provide certificates for LDAP server. The connection to the LDAP server is a plain text transmission. Therefore the security attributes will not be changed.

Key Management

The trustworthiness of the CA is based on the public key of the Certification Authority, which is permanently stored within the TOE, as well as the TOE's key-pair. The TOE is able to monitor the integrity of those internally stored keys and switches to a secure state in case a integrity error was detected. The TOE key-pair (especially the private key) can only be created and deleted by the Administrator. The TOE provides the generation of RSA key pairs with module length of 1024 or 2048 bit according to the ANSIX9.31 criteria for RSA. The TOE provides also mechanisms to destroy the local platforms key-pairs by zeroisation. The CA's public-key can only be imported and stored by the Administrator.

Verification of Signature

The signatures of the Certification Authority over the certificates and the certificate revocation list (CRL) are checked by the TOE. The TOE has to check the integrity of the CRL by the successful verification of its signature using the algorithms RSA (with a key length of: 1024 or 2048 bit, according to PKCS #1:RSA Encryption Standard) and SHA (according to FIPS PUB 180-1) ensuring that the CA is the originator. In case an invalid signature was found, the CRL will not be accepted; otherwise the TOE verifies the validity, and the timestamp of the CRL for up-to dateness. The TOE verifies the signature of the X.509 certificate for correctness with the public key of the CA using RSA with the specified key length and SHA-1 ensuring that the CA is the originator. In case an invalid signature was found, the certificate will not be accepted; otherwise the validity of the certificate will be checked. This implies the check of the time of validity and that the Certificate Serial Number is not rejected by the current certificate revocation list. Invalid, rejected or corrupted certificates won't be accepted. In case that no current CRL is available on the TOE no certificate can be checked and accepted.

To get more details refer to the Security Target [6], chapter 6.1.

1.3 Strength of Function

The TOE's strength of function is rated 'SOF-basic'.

There are two identified probabilistic or permutational mechanisms:

- the password mechanism for the User identification and authentication,
- a pseudo (deterministic) random number generator (PRNG) used for key generation and challenge generation during the SSL handshake. This mechanism was assessed according the AIS20.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

A summary of the threats defined in [6], chapter 3.6 is provided here. For the precise description of the threats please refer to Security Target:

T.RP_Data: **Modification or eavesdropping of communication data during transfer**

A net-attacker modifies or eavesdrops the content of a RP-data during the transfer, between the TOE and a remote platform, to achieve unauthorised information or to violate the integrity of RP-data.

T.Mobile_Agent: **Modification or eavesdropping of mobile agent data during transfer**

A net-attacker modifies or eavesdrops the content of a mobile agent during the transfer, between the TOE and a remote platform. This threat enables the net-attacker to achieve unauthorised information about the mobile agent data or to violate the integrity of the mobile agent. Furthermore modification of a mobile agent enables the net-attacker to manipulate the functionality (i.e. executable code) in such an illicit way that threatens the platform integrity.

T.User_data: **Modification or eavesdropping of user data during transfer**

A net-attacker modifies or eavesdrops user data which is transferred, between a trustworthy user interface and the TOE, to achieve unauthorised information or to violate the integrity of user data. User data comprise identification and authentication data and user application data.

T.CA_Data: **Modification of certificates or the certificate revocation list (CRL) during transfer**

A net-attacker modifies CA-data (certificates or CRLs) which are transferred between a Certification Authority and the requesting platform.

The TOE has to comply to the following Organisational Security Policies (OSPs). Note that only a summary of the policies is provided here. For the detailed and precise definition refer to the Security Target [6], chapter 3.7:

P.RP_Communication: **Communication with trustworthy platforms**

The TOE has to ensure that RP-data and mobile agent data are only sent and received between itself and trustworthy remote platforms.

P.UI_Communication: **Communication with trustworthy user interfaces**

The TOE has to ensure that user data (identification and authentication data, and user application data) is only sent and received between itself and trustworthy user interfaces.

P.LDAP_Communication: **Communication with LDAP**

All plain text data received by the TOE will only be accepted as LDAP registration information. Only agent registration information to a LDAP will be sent as plain text data by the TOE.

P.CA_Communication: **Communication with Certification Authority**

The TOE has to ensure that only CA data (valid certificates and CRLs) generated by the Certification Authority are accepted.

1.5 Special configuration requirements

The TOE gains and obtains its resources by the runtime environment that is realised by the Java Virtual Machine (version 1.4.2_04). The purpose of the runtime environment is to provide access to the host system resources and to act as an interface between the local agent platform and the underlying operation system. Other hardware or software requirements are not demanded.

1.6 Assumptions about the operating environment

The following constraints concerning the operating environment are made (see [6], chapter 3.5):

A.CA_Cert: CA generates platform certificates and a certificate revocation list (CRL)

The trustworthiness of remote platforms and user interfaces is given by a Certification Authority (CA) that provides certificates over these platforms. The Certification Authority is also responsible for validity, up-to-dateness, and reliability of the list entries and provides a certificate revocation list. The CA uses strong cryptographic mechanisms and appropriate key lengths to generate unforgeable signatures.

A.User_Interface: Trustworthy user interface for application creation

The trustworthy user interface ensures that only user identification and authentication, and user application data is transmitted to the TOE. The user interface also ensures integrity and confidentiality of UI-internally transferred user data. The user interface provides adequate mechanisms to facilitate secure communication.

A.Remote_Platform: Trustworthy remote platform

The trustworthy remote platform solely sends speech act and mobile agent data. These data do not contain any malicious or illicit data. The platform provides adequate mechanisms to facilitate secure communication.

A.Access: Limited physical access and logical access

The direct physical access to the TOE (i.e. to hardware, OS and the platform) is limited to authorised persons (Administrator) only. Also the direct physical access, protected by an OS identification and authentication mechanism, is the only way to administer the TOE. Also the IT-Environment (HW, OS) has to ensure the protection of the resource used by the TOE against external attacks.

1.7 Disclaimers

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 is called:

Java Intelligent Agent Componentware IV

(JIAC IV),

Version 4.3.11

The TOE is represented by the JIAC agent framework, the AMS, the SA, and the AE that are all parts of the seller platform.

The TOE is delivered in a signed zip archive which contains several components:

- all documents (administrator guidance) that the TOE contains necessarily
- the necessary jar (java archives) files of the TOE that were developed by the DAI-Labor and
- the needed third party libraries

The zip archive is called:

JIAC-IV_Cert_4_3_11.zip.

The SHA-1 value of the zip archive is calculated as

42e731e549e6d1f54639e6090b3b9f96b93f4412

The zip archive includes the following jar files:

Developed by the DAI-Labor:	**last modification**	**CRC32**
cat.jar	2004/12/08	BC63C8DE
control.jar	2004/12/08	1DF16831
cryptoiaik.jar	2004/12/08	1963DC34

daigui.jar	2004/12/02	1BDED0F8
jiac-conf.jar	2004/12/08	E263041C
jiac.jar	2004/12/08	B487065C
kit.jar	2004/12/08	943DF4AB
navigator.jar	2004/12/08	41D4E339
ontocompiler.jar	2004/12/08	445CBFDE
security.jar	2004/12/08	36042B0A
util.jar	2004/12/08	79CDF10C
Third party libraries:		
ldapjdk.jar	2004/12/02	8246ACFA
iaik_jce_full.jar	2004/12/02	D3159C8E
iaik_ssl.jar	2004/12/02	0AD30373
PwdManager.jar	2004/12/08	03B24069
trading_seller.jar	2004/12/08	64B541CC
TradingGUI.jar	2004/12/08	F5A48EBB

table 2: Delivered .jar files

The following guidance document is supplied together with the TOE. The guidance document has to be followed to ensure an certification conformant operation of the TOE:

- Administrator Manual, Version 2.7, November 30th 2004 [8]

3 Security Policy

The intended use of the TOE is to handle and protect services against obvious vulnerabilities during external communication to other (trustworthy) entities and on the local platform against attacks initiated from the network.

Therefore the TOE ensures that remote platform data, mobile agent data and user data are only sent and received by itself and trustworthy remote platforms and user interfaces. Furthermore only CA data generated by the Certification Authority are excepted by the TOE. All plain text data will only be accepted as LDAP agent registration information.

4 Assumptions and Clarification of Scope

4.1 Usage assumptions

Based on the personnel assumptions the following usage conditions exist. Refer to [6], chapter 3.5 for more details:

- The direct physical access to the TOE is limited to authorised persons (Administrator) only (A.Access).

4.2 Environmental assumptions

The TOE runs on the Java Virtual Machine (version 1.4.2_04).

Based on the assumptions on the environment the following conditions exist. Refer to [6], chapter 3.5 for more details:

- The direct physical access protected by an OS identification and authentication mechanism is the only way to administer the TOE (A.Access).
- The trustworthiness of remote platforms and user interfaces is given by a Certification Authority (CA) that provides certificates over these platforms. The CA is also responsible for validity, up-to dateness and reliability of the Certificate revocation list. The CA uses strong cryptographic mechanisms and appropriate key lengths to generate unforgeable signatures (A.CA_Cert).
- The trustworthy user interface ensures that only identification and authentication data and user application data are transmitted to the TOE. The user interface also ensures integrity and confidentiality of internally transferred user data. The user interface provides adequate mechanisms to facilitate secure communication (A.User_Interface)
- The trustworthy remote platform solely sends speech act and mobile agent data. These data do not contain any malicious or illicit data. The platform provides adequate mechanisms to facilitate secure communication (A.Remote_Platform).

4.3 Clarification of scope

There are no threats that have to be averted in order to support the TOE security capabilities but are not addressed by the TOE itself.

5 Architectural Information

The general structure of the TOE consists of the underlying abstract functionality given by:

1. The JIAC IV agent framework that realises the execution components that are basic to all agents, further the JIAC IV meta-protocol, control of JADL services, generation of good pseudo-random numbers, as well as cryptographic verification methods to handle X.509 certificates;
2. The agent management system (AMS) that provides local white pages and global agent yellow pages, the agent communication channel and migration services, external communication interfaces such as TCP/IP and SSL, and management (creation, usage, and zeroisation) of the locally stored asymmetrical key-pair;
3. The security agent (SA) is responsible to request certificates and a CRL from the CA and to provide the KeyDistributionCenter where X.509 certificates can be managed, also the SA handles TrustRelationships to other remote platforms where local agents can migrate to; and finally the
4. Alter Ego Agent (AE) that serves creation, storage and deletion of user identification & authentication data and thereby also realises the service interface to any trustworthy (human) user interface, including handling of user application data by the generic GUI service, offered by the AE.

An overview of the identified TOE subsystems together with the corresponding TOE interfaces can be found in the following figure:

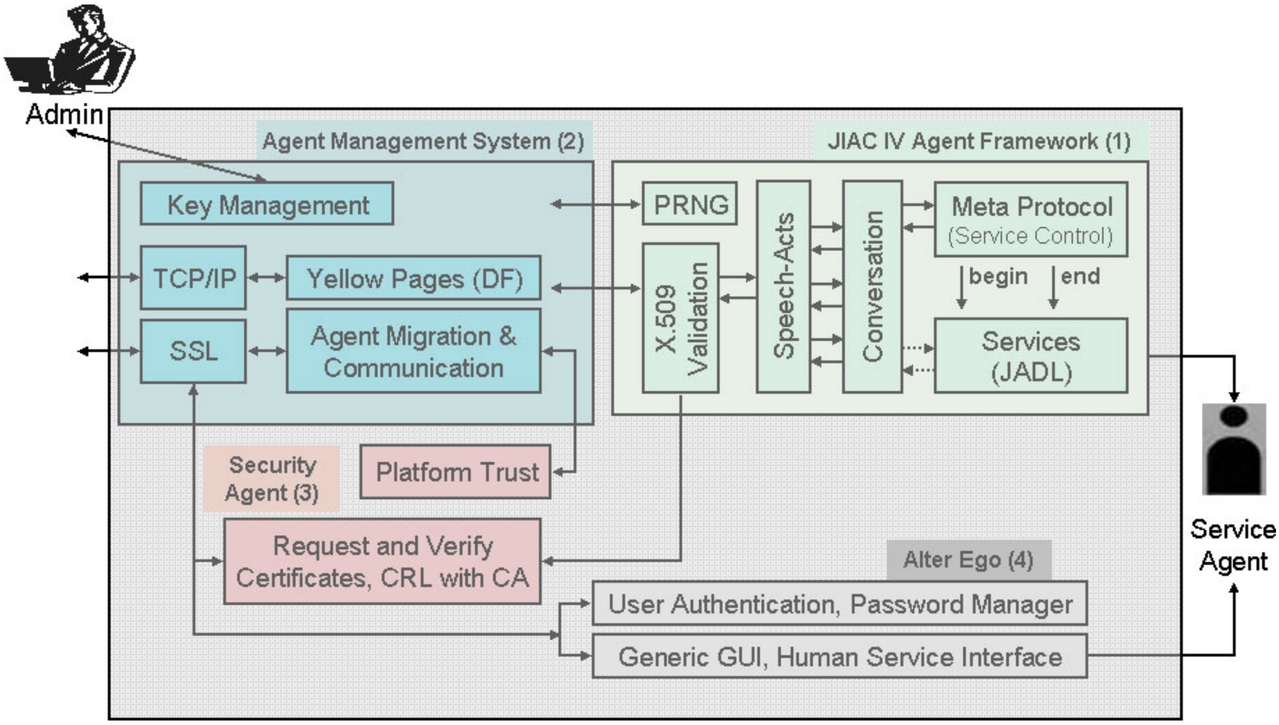
Admin
Agent Management System (2)
JIAC IV Agent Framework (1)
Key Management
TCP/IP
Yellow Pages (DF)
SSL
Agent Migration & Communication
PRNG
X.509 Validation
Speech-Acts
Conversation
Meta Protocol (Service Control)
begin
end
Services (JADL)
Security Agent (3)
Platform Trust
Request and Verify Certificates, CRL with CA
Alter Ego (4)
User Authentication, Password Manager
Generic GUI, Human Service Interface
Service Agent

figure 1: TOE subsystems and interfaces

Subsystem 1: The JIAC IV Agent Framework

The JIAC IV Agent Framework cannot be seen as an agent explicitly in contrary to the other subsystems, which are all JIAC IV agents. The functionality of the JIAC IV agent framework can be considered as abstract functionality, meaning that they do not realise any explicit functionality as much more a public interface that is usable by all agents and therefore accessible to the complete JIAC IV Agent Componentware. In the following the functionality of the Subsystem 1: The JIAC IV Agent Framework is described according to it's main points:

- Usage of the meta-protocol and control of JADL services that are required to be checked before any service provided by an agent can be used.
- Validation of CRL and X.509 certificates, which is realised by the X509ValidationComponent that handles methods for validating certificates and CRLs.
- Generation of pseudo-random numbers to support the strength of cryptographically executed TOE operations.

(a) JIAC IV Meta-Protocol

Service-based conversations (Agent Services) are based on the fact that the co-ordination of conversations, respectively of all agent communication processes in JIAC are realised by services that consist out of a user and a provider side. These Services are managed by the meta-protocol.

(b) Control of JADL Services

The ServiceControlMechnismsBean is used to control access to services offered to other agents. Each agent (AMS, SA, and AE), has a ServiceControlMechanismsBean, as part of its set of security components.

The access control policy is configured with properties for the component. Further more service control lists (SCL) are used for a fine grained access control policy. In the TOE they are used to forbid access to services, that are normally offered by an AMS, ACC, DF, Security Agent or Alter Ego Agent, but are not needed/wanted to be available in the TOE.

The access control to agent services in JIAC IV consists of two parts. First, the SSL component verifies that the communication partner is allowed to request the use of a service this is done by validating a presented X.509 certificate. Second, after a successful certificate validation by the SSL component, the service control component checks if the requested services can be used. This mechanism is realised by the verification of the incoming entity with an already specified service control list.

(c) Generation of Pseudo Random Numbers

Random numbers are important for cryptography. But computers are not very good at producing truly random data, because they must rely on a pseudo-random number generator (PRNG). Such a cryptographically strong PRNG should be seeded with truly random values.

The initial seed will be generated newly during every start of each agent platform by a further specified algorithm producing random data from mouse movement events. The input of the user will be started by a modal dialog with a progress bar that shows how far along the generation is. The generated seed will be hold temporally in the fact base of the AMS only and will be iterated for use in a specified cycle.

(d) Validation of CRL and X.509 Certificates

Before any SSL connection can be established to other entities, such as a trustworthy remote platform, user interface, or certification authority it is required that the transport component of the AMS validates the exchanged X.509 certificates.

The X509ValidationComponent handles the validation of X.509 certificates and X.509 CRLs.

Certificate and CRL management components:

- The KeyDistributionCenter (realised by the KDCBean) used as a register for storing certificates and the CRL
- Updates, e.g. pulling the CRL from the CA, of the KDCBean
- Management, updates and validation of certificates

The validation of certificates is an essential part of the SA functionality. But in contrast to the SA subsystem the X509ValidationComponent is usable by other agents as well, thus ist functionality is best represented as within this subsystem. If the CRL verification was not successful the according meta-protocol will be terminated and will not result in an established connection.

Subsystem 2: The Agent Management System

The functionality of the Agent Management System, in the following AMS, the platform manager of a JIAC IV platform, are listed as follows:

- TCP/IP in the meaning of LDAP-based data exchange, which is carried out via the DF interface.
- SSL communication to exchange:
    - CRLs as requested by the SA and certificate data with a CA
    - speech-acts and mobile agents with a trustworthy remote platform
    - user identification and authentication as well as user application data that is requested by the AE with an authenticated trustworthy user interface
- Management of Internally Stored Keys

(a) The Directory Facilitator (DF)

The DF component communicates with an LDAP server via a TCP/IP connection. The modification of security attributes "trusted SSL connect" (no) and "role" (none) can only be changed in accordance with a successfully established SSL connection but not with TCP/IP.

(b) The SSL Communication Interface

Basically the AMS possesses only two means to communicate with other agents. First, it can use the internal transport component, which is based on the Java Virtual Machine communication methods. This component allows communication with all agents within the same Java Virtual Machine.

Second, it has the possibility to use the component OnlyDefaultCipherSSLCommunicationBean. This component enables the AMS to establish connections to other agents with SSL transport components. Additionally it has to be mentioned that the DF part of the AMS can communicate via plain text TCP/IP but this does not influence the secure SSL communication channel.

(c) The Migration Service

Migration is a service provided by the AMS to any agent on its platform, which basically provides a secure transmission of mobile agents between the TOE and trustworthy Remote Platforms. Using this service any agent can search for a trustworthy RP. Then the AMS verifies the target address, the migration process and the accessibility of the destination platform. The structure of the secured migration protocol is not equal to the plain migration protocol although it is primarily based on it. It is important to note that the migration service for sending an agent from a source to a destination platform works and describes the very same as if the source platform would receive a mobile agent. Therefore this process is only described once.

Further, as in this scenario mobile agents are only used based on an user initiated service, they always carry an unique service-ID that helps to map the user on the Navigator platform to the currently used service and the corresponding (mobile) service agent that acts upon the user request. This service-ID is a simple string and can only be interpreted correctly by the AE agent.

(d) Management of Internally Stored Keys

Management of internally stored keys deals with the creation, storage, and deletion of secure data, which are: the asymmetrical AMS key-pair as well as the password used to protect the TOE private key and finally there is the public key of the CA.

On one hand it is required to configure the asymmetrical key-pair of the (local) AMS agent, so that specific certificate based SSL communication is possible with trustworthy CA, UI, and RP.

On the other hand it is absolutely necessary to import the public key of the CA, so that X.509 certificates of remote platforms can be verified and validated along with the signature that was provided by the CA. The counterchecking of the CA's public key must be fulfilled by the platform administrator.

Furthermore he is the only person who can change the CA certificate afterwards by having physical access to the host machine.

Subsystem 3: The Security Agent

The Security Agent, in the following SA, provides three main functions:

- Firstly the SA interprets the interactions, by using the SSL communication component of the AMS, with a Certification Authority (CA) to request certificates and a CRL.
- Secondly the SA verifies the trustworthiness of a X.509 certificate. The result is used by the Agent Management System (AMS) which decides if the communication process shall be continued or aborted.
- Finally the SA verifies, in case an agent wants to migrate to a remote platform, the required level of trust from the provided X.509 certificate.

In the following the interfaces of the SA will be identified in accordance of how the SA realises security functionality.

The SA requires the X509ValidationComponent from Subsystem 1.

(a) Receiving the CRL and Certificates from a CA

The main purpose of the certificate management component is to store certificates and private keys in the fact base of the security agent. From the moment when the certificates are part of the agent’s fact base, they can be accessed by any agent. On the other hand the private key of the agent stays in its fact base for local usage only.

It needs to be mentioned that the interface to the CA is effectively realised between the CA and the AMS, with which the SA is communicating. This is because only the AMS of the local platform is able to initiate and use a secure communication channel (SSL) with a remote entity, such as the CA. The internal interface of the SA that is transmitted via the AMS consists out of two services to receive the certificates and the CRL that were published by the CA.

Furthermore the internal component of the SA to request a list of published certificates and a CRL from the CA continuously is realised within the UpdatingKDCBean component that requests certificates and the CRL from a CA and offers it to local agents needing to verify a X.509 certificate.

(b) Interfaces to every JIAC Agent to retrieve and validate certificates

The interface to the local agents can be separated into the following three:

- The PublishCertificatesService service is offered by the SA to other agents so that they can retrieve certificates that the SA validated successfully before.
- The ValidateCertificateService service is offered by the SA to other agents so that they can verify certificates based upon a valid CRL.
- In the service KDCRequestCRLList the SA serves as a mediator between the CA and any agent on the local platform to forward an actual and valid CRL.

The underlying base of this functionality is realised within the certificate management component, which main purpose is to store certificates and private keys in the fact base of the security agent. From the moment on the certificates and private keys are part of the agents fact base, they can be used by the agent. The sources of certificates are the properties mentioned above or the interface UpdatingKDCBean. The UpdatingKDCBean sends an agent internal message to the CertificateManagementBean, if it has requested a certificate list and received a valid result. Before certificates are added to the agents fact base the CertificateManagementBean ensures, that only allowed certificates are added. The functionality for validating certificates is inherited from the interface X509ValidationComponent. If a certificate failed the validation a log entry will be created and the certificate will be not imported..

(c) Interfaces during agent migration

The following interfaces are used in compliance with the AMS that actually is trying to either send or receive a mobile agent:

- The trust provider component is used for managing trust relationships between agent platforms for migrating mobile agents. For any agent platform one of the following values may be assigned: trusted, migrate_to, migrate_from, untrusted, and unknown. All trusted values are collected in a MTL (Marketplace trust list) and stored in the fact base of the SA.
- The QueryTrustForMarket service that locally verifies if the remote platform belongs to a list of trusted market places (respectively platforms).

- The RequestMTL service where any agent can request the complete MTL.

Subsystem 4: The Alter Ego Agent

The responsibility of the Alter Ego agent lies in the establishment of a secure channel to a trustworthy user interface that is in fact carried out by the AMS. Therefore to connect to the user side of the TOE, whose functionality is constituted within the Alter Ego (AE) component, first of all a trusted user needs to be authenticated with an account management component.

If the authentication process was successful the AE will provide a list of usable services that a human user can use. This concept is realised by the generic GUI concept. The generic GUI concept comprises the following components:

- Interface to receive and send user identification and authentication data.
- User application data such as the service-ID that needs to be included within the mobile agent when it is acting upon the requested service of an user.
- Interface to the AMS to exchange data on request of the mentioned interfaces.

Following a successfully verified and registered user can initiate and use the services that are provided by the TOE. These services can either be carried out locally on the TOE platform or use further more a mobile agent scenario. When a mobile agent, based upon an initiated user service, migrates to a remote platform it is always required to carry a unique service-ID that the AE agent can always map to the user that initiated that service. This allows the interpretation of the results of the mobile agent according to the currently used service and the processing of the results to the user side.

The AE subsystem provides the DFHumanService and the AuthGenericGUIService.

(a) The Password Manager

For human users the management of identification and authentication data is required. This functionality is provided by the TOE's password manager. Whereas the first password for a new user can only be generated by the platform administrator, the human user, once identified and authenticated successfully, can modify his password anytime he wants to.

But changing the password the first time a user logs in, is compulsory. This is aimed at making sure that critical user data is known to the user and only to them.

Organisationally the administrator sends the account data through a trusted channel to the user and the user must be able to adjust it to its own secrets. Due to the account manager the platform restricts the ability to modify the internally stored user authentication data belonging to the identified user. Verification and enforcement processes of pass-phrases (authentication data) with a minimal length of eight alphanumerical characters are also carried out within the password manager.

(b) Overview of the service usage process

The next section takes a closer look to the internal functions of the “GenericGUIService” between the (human) user interface and the AE.

This interface describes the communication process between the user-side and the TOE. The AE performs the translation process so that the intended user behaviour can be mapped and used by the offered JIAC agent services. As already mentioned it is necessary to understand the AE agent not communicating directly with the user interface as much more communicating with the AMS residing on the same platform. This is due to the fact that the AMS is the only entity that can establish outside communication channels. The protocol is able to handle messages (results) provided by the service provider and requests by the human user at the same time. This is established via synchronous handling and usage of message queues.

Confidentiality of written password data is ensured by using the one-way secure hashing algorithm SHA -1.

Basically the Navigator GUI consists of the platform manager and the GUI component. The platform manager is able to communicate with other platforms whereas the GUI component is only responsible for providing an interface between the platform manager and its defined environment, which is the interface to the human user. The human user can request services from an initiated AE agent that serves as a provider. It is the Navigator‘s aim to receive a .jar file that contains the graphical user interface to initiate that specific service. After that the generic GUI protocol will be processed and install the user interface within the accessible Navigator frame. Therefore every time the user selects one of the services the Navigator platform requests the GUI-jar file from the (TOE) AE agent and if received correctly it will be represented in the right side of the Navigator window in an internal frame. The matching of services with users is accomplished by the AE agent that holds an internal database about the actual list of connected users to the accessible services. All other parameter for correct service usage have to be / can be configured within the provided service GUI. If so the service will be initiated.

Each service usage starts by discovering human usable agent-based services offered by the TOE. Basically within the TOE a human service is not separable from other TOE provided services. The only difference is when the LDAP server, as a global yellow page directory, receives and stores services provided for (human) users as "human" services. These human services are only usable by human users because their basic functionality is implemented within the AlterEgo to Navigator concept.

This means that, even though the AMS receives and forwards the communicated data, as it is the only external interface for establishing a secured communication channel, to the DF and to the AE. Since the DF agent stores this service list, the user interface of the navigator agent asks the DF-Agent of the TOE by using the service “DFHumanService”.

6 Documentation

Documentation provided with the product by the developer to the consumer is the „Administrator Manual – Das Administrationshandbuch der lokalen Plattform“, Version 2.7 from November 30th 2004 [8].

7 IT Product Testing

7.1 Developer Testing

Test configuration:

The tested version of JIAC IV in all documents equals to JIAC-IV_Cert_4_3_10. The following tables represent a specified view on the configured Hardware and installed Software on each test system.

Test System	Hardware	Software
RedHat Linux	Processor: 2400MHz Intel	JIAC BuildSystem (JIAC-IV_Cert_4_3_10)
	1GB Memory	Java (TM) 2 Runtime Environment, Standard Edition, (build 1.4.2_04-b05)
	32 Bit Operating System	Java HotSpot (TM) Client VM (build 1.4.2_04-b05, mixed mode)
	37,27 GB Hard drive	JCE Unlimited Strength Crypto API v 1.4.2 ('local_policy.jar' and 'US_export_policy.jar')
SUN Solaris 9 SUN OS Release: 5.9	Processor: 2400MHz Intel	JIAC BuildSystem (JIAC-IV_Cert_4_3_10)
	1GB Memory	Java (TM) 2 Runtime Environment, Standard Edition, (build 1.4.2_04-b05)
	32 Bit Operating System	Java HotSpot (TM) Client VM (build 1.4.2_04-b05, mixed mode)
	38,17 GB Hard drive	JCE Unlimited Strength Crypto API v 1.4.2 ('local_policy.jar' and 'US_export_policy.jar')

Microsoft Windows XP Professional, Version 2002, Service Pack 1	Processor: 2400MHz Intel	JIAC BuildSystem (JIAC-IV_Cert_4_3_10)
	1GB Memory	Java (TM) 2 Runtime Environment, Standard Edition, (build 1.4.2_04-b05)
	32 Bit Operating System	Java HotSpot (TM) Client VM (build 1.4.2_04-b05, mixed mode)
	37,27 GB Hard drive	JCE Unlimited Strength Crypto API v 1.4.2 ('local_policy.jar' and 'US_export_policy.jar')

table 3: Hard- and Software on test systems

The testable configuration of the TOE comprises an e-Business scenario implemented by Service agents acting on the platform, which are not part of the evaluation.

Testing effort:

The tests were separated into the following seven groups of test classes:

- User management tests mainly address SF1.4.
- Graphical user interface tested on the user login and the verification of the user interface, therefore address SF1.2 and SF1.4.
- Communication tests address the correct functionality and implementation of establishing SSL connections in SF1.1; SF2.1; SF4.1; and SF5.1. Also this addresses the platform management SF1.5; SF2.4; SF3.3; SF4.4; and SF5.6.
- Access control tests are used to test the prohibition of certain services and addresses SF1.3; SF2.3; F4.3; and SF5.4.
- Secure DF tests encounter the SF3.1; SF3.2; and SF3.3.
- Migration tests are used to verify the correct transmission of a migrating agent and addresses SF4.2. This coherently tests also the SF2.2. Certificate and key management tests address the handling of keypairs as in SF5.3, the communication to request certificates as in SF5.2 and SF5.5.

For further information about tested Security Functions refer the Security Target [6].

Test results:

The developer has provided a complete specification of the test activities with further descriptions of the test results, such as error descriptions, taken measures, a description on the test actions and upcoming side effects during testing.

All tests were passed successfully.

7.2 Evaluator Testing

The evaluators examined the developer's test plan to determine, that the test configuration is consistent with the configuration identified for evaluation in the Security Target [6]. The evaluators also examined the coverage and depth evidence and they determined, that the correspondence between the tests identified in the test documentation, the functional specification and the high level design is correct and complete.

The evaluators have reproduced a subset of developer tests using the test configuration and test specification described in chapter 7.1. As a test strategy the evaluators decided to test the security functions as complete as possible:

Security Function	Reproduced developer tests
SF1: User communication	84 (99%)
SF2: Remote platform Speech-act transmissions	37 (100%)
SF3: LDAP based data exchange	1 (100%)
SF4: Mobile agent transmission	65 (98%)
SF5: Certificate and key management	62 (72%)

table 4: Coverage of repeated developer tests

The evaluators have furthermore developed and performed 29 additional test cases to increase the confidentiality into the TOE.

All tests were passed successfully.

The only difference between the version JIAC-IV_Cert_4_3_10 and JIAC-IV_Cert_4_3_11 is the version of the administrator manual . The source code of the TOE did not change. The evaluators examined the differences between the tested (JIAC-IV_Cert_4_3_10) and the delivered TOE (JIAC-IV_Cert_4_3_11) and determined that the differences are not security relevant. So the test results are still valid.

8 Evaluated Configuration

The TOE is the JAVA Intelligent Agent Componentware IV, version 4.3.11, shortly called JIAC IV. The software is stored within a signed downloadable package JIAC-IV_CERT_4_3_11.zip. The TOE runs on a JAVA virtual machine (version 1.4.2_04) on different operating systems like Windows, Linux or Sun Solaris as outlined in chapter 7. The purpose of the runtime environment is to provide access to the host system resources and to act as an interface between the local agent platform and the underlying operation system. Other hardware or software requirements are not demanded.

For further details about the tested configuration refer chapter 7.

9 Results of the Evaluation

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

The verdicts for the CC, Part 3 assurance components are summarised in the following table:

Assurance Classes and Components		**Verdict**
Security Target	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Authorisation controls	ACM_CAP.3	PASS
TOE CM coverage	ACM_SCP.1	PASS
Delivery and Operation	CC Class ADO	PASS
Delivery Procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Identification of security measures	ALC_DVS.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-level design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS

Assurance Classes and Components		Verdict
Vulnerability assessment	CC Class AVA	PASS
Examination of guidance	AVA_MSU.1	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

table 5: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 conform,
- the assurance of the TOE is Common Criteria Part 3 conformant according to EAL3,
- the following TOE Security Functions fulfil the claimed Strength of Function:
  - the password mechanism for the User identification and authentication,
  - a pseudo (deterministic) random number generator (PRNG) used for key generation and challenge generation during the SSL handshake. This mechanism was assessed according the AIS20 [4].

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for the cryptographic mechanisms 3DES, RSA and SHA-1.

The TOE has no obvious vulnerabilities which are exploitable in the intended operating environment.

The results of the evaluation are only applicable to the product JAVA Intelligent Agent Componentware IV, Version 4.3.11 in the configuration as defined in the Security Target, on Java platform used for testing and the comments and recommendations outlined below taken into account.

The validity can be extended to new versions and releases of the product or for new platforms, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and if the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The operational documentation [8] contains necessary information about the download, verification, installation and usage of the TOE which has to be followed. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment resp. the security requirements for the IT and non-IT environment as outlined in the Security Target have to be taken into account.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

AE	Alter Ego
AMS	Agent Management System
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security
CA	Certification Authority
CC	Common Criteria for IT Security Evaluation
CRL	Certificate Revocation List
DF	Directory Facilitator
EAL	Evaluation Assurance Level
IT	Information Technology
JADL	Java Agent Description Language
JIAC	Java Intelligent Agent Componentware
KDC	Key Distribution Center
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PP	Protection Profile
PRNG	Pseudo Random Number Generator
SA	Security Agent
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
SSL	Secure Socket Layer

ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
UI	User Interface

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 entity within the TSC that contains or receives information and upon which subjects perform operations.

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

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

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

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

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

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

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

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

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

[6] Security Target Java Intelligent Agent Componentware IV, version 3.0, Nov 30th 2004 , DAI- Labor, Salzufer 12, 10587 Berlin

[7] Evaluation Technical Report, version 1.2, date: 09th December 2004, (confidential document)

[8] Administrator Manual, JIAC-IV, version 2.7, date: 30th November 2004

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Caveats on evaluation results (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

Part 2 conformant - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

Part 2 extended - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

Part 3 conformant - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

Part 3 extended - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

Assurance categorisation (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

Assurance Class	Assurance Family	Abbreviated Name
Class ACM: Configuration management	CM automation	ACM_AUT
	CM capabilities	ACM_CAP
	CM scope	ACM_SCP
Class ADO: Delivery and operation	Delivery	ADO_DEL
	Installation, generation and start-up	ADO_IGS
Class ADV: Development	Functional specification	ADV_FSP
	High-level design	ADV_HLD
	Implementation representation	ADV_IMP
	TSF internals	ADV_INT
	Low-level design	ADV_LLD
	Representation correspondence	ADV_RCR
	Security policy modeling	ADV_SPM
Class AGD: Guidance documents	Administrator guidance	AGD_ADM
	User guidance	AGD_USR
Class ALC: Life cycle support	Development security	ALC_DVS
	Flaw remediation	ALC_FLR
	Life cycle definition	ALC_LCD
	Tools and techniques	ALC_TAT
Class ATE: Tests	Coverage	ATE_COV
	Depth	ATE_DPT
	Functional tests	ATE_FUN
	Independent testing	ATE_IND
Class AVA: Vulnerability assessment	Covert channel analysis	AVA_CCA
	Misuse	AVA_MSU
	Strength of TOE security functions	AVA_SOF
	Vulnerability analysis	AVA_VLA

Table 2.1 -Assurance family breakdown and mapping“

Evaluation assurance levels (chapter 6)

„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 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 6.1)

Table 6.1 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 2 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

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

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6.1 - Evaluation assurance level summary“

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 6.2.1)

„Objectives

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

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

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.“

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 6.2.2)

„Objectives

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

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

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 6.2.3)

„Objectives

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

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

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 6.2.4)

„Objectives

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

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

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 6.2.5)

„Objectives

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

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

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 6.2.6)

„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 6.2.7)

„Objectives

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

Strength of TOE security functions (AVA_SOF) (chapter 14.3)

AVA_SOF Strength of TOE security functions

„Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim."

Vulnerability analysis (AVA_VLA) (chapter 14.4)

AVA_VLA Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users."

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis."

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential."

This page is intentionally left blank.