SECURITY TARGET

Java Intelligent Agent Componentware IV

Version 3.0

Revision date Nov 30th, 2004

Revision history

Version	Date	Changes	Remarks
1.0	Jun 17th, 2003	Official Draft (based on JIAC-IV_Cert_ST_062.doc)	JW, TG
1.1	July 4th, 2003	Changes on format style and editorial inconsistencies	TG
1.2	July 17th, 2003	Final changes for evaluation version	TG
1.3	July 23rd, 2003	Minor changes on expressions of SFR and SF	JW, TG
1.4	July 28th, 2003	Changes on expression of service description and SF supportiveness.	TG
1.5	July 30th, 2003	Minor changes on R.Restricted_Access	JW
1.6	Nov 24th, 2003	Revision on TOE description, threats, assumptions and policies, added assets, FIA_UAU.1, list of figures, and list of tables	JW, TG
1.7	Nov 26th, 2003	Updated date and version nr, revised security objectives and physical boundary of the TOE	TG
1.8	Dec 19th, 2003	Format style revision and document change due to change request from Dec 16th	TG
1.9	Jan 05th, 2004	Updated table of contents (pg. nr.)	TG
2.0	Jan 05th, 2004	Updated year to 2004	TG
2.1	Feb 13th, 2004	Update according Review Report (BSI)	JW
2.2	Feb 17th, 2004	Verification of last update	TG
2.3	Feb 26th, 2004	Applied new SF structure and added FIA_UAU and FIA_UID for entity	JW
2.4	Mar 10th, 2004	Revised last document changes, updated IAIK versions	TG
2.5	Mar 25th, 2004	Added extra information for Management Functions in the TSS	TG
2.6	May 25th, 2004	Added A.Remote_Platform and adequate rationale	JW
2.7	May 26th, 2004	Revised document changes	TG
2.8	Aug 19th, 2004	Adjusted copyright for publication	TG
2.9	Aug 20th, 2004	Modified SR for IT env. due to RI#58	TG
3.0	Nov 30th, 2004	Updated TOE version	TG

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

Copyright

Document Organisation

The document is organised according to Common Criteria, Part 1: Introduction and general model [1], Annex C.

Invariant of the document

Invariant	Value	Show Value
name and file length	automatically set	JIAC-IV_Cert_ST.doc (1329664 Byte)
last version	Version 3.0	Version 3.0
date of this version	Nov 30th, 2004	Nov 30th, 2004
confidentiality	Company-confidential	Company-confidential
name of the TOE (short)	JIAC IV	JIAC IV
name of the TOE (long)	Java Intelligent Agent Componentware IV	Java Intelligent Agent Componentware IV
developer (long)	DAI-Labor TU Berlin, Fakultät IV Salzufer 12, D-10587 Berlin	DAI-Labor TU Berlin, Fakultät IV Salzufer 12, D-10587 Berlin
developer (short)	DAI-Labor	DAI-Labor
Registration number	BSI-DSZ-CC-0248	BSI-DSZ-CC-0248

1. ST Introduction

1.1. ST identification

Title:	Security Target Java Intelligent Agent Componentware IV
Authors:	DAI-Labor TU Berlin, Fakultät IV Salzufer 12, D-10587 Berlin
General Status:	official
CC Version:	2.1 Final, incorporated with interpretations as of 2002
Version Number:	Version 3.0, Nov 30th, 2004
Registration:	BSI-DSZ-CC-0248
Keywords:	telecommunication services, mobile agents, framework

1.2. ST overview

The TOE is the Java Intelligent Agent Componentware IV developed by the DAI-Labor. JIAC IV is now in its actual version 4.3. JIAC IV is suitable for business, telematic, and telecommunication services.

In the following, agents are understood as software systems that are managed by a specific multi-agent platform. Agents are capable to act autonomously and flexible to realise specified services. The agent platform gains and obtains its resources by the runtime environment that is realised by the Java Virtual Machine (version 1.4.2_04). Therefore the runtime environment can be understood as the underlying layer of the agent platform. Further more every platform is connected to other agent platforms by a network of trustworthy platforms.

To offer scalability and flexibility the principle concept of JIAC IV is based on knowledge and interaction via service agents that can be differentiated by the following two kinds:

(i) Infrastructure agents that must reside stationary. These agents include management agents to support maintenance and security functionalities. They are under the sole control of an Administrator.

(ii) Application service agents, acting as an application service accessible to other agent platforms or directly on behalf of a (human) user and can be initiated and handled by a graphical user interface.

Agent platforms can transfer speech acts, as in the meaning of Remote Platform data, to update information on service application data or simply to use a service. Furthermore this includes mobile agents that are able to migrate from one platform to another on behalf or as part of a service.

1.3. CC conformance

The ST is Common Criteria, Part 2: Security functional requirements ([2]) conformant and Common Criteria, Part 3: Security assurance requirements ([3]) conformant.

The assurance level for this ST is **EAL3** conformant. The minimum strength level for the TOE security functions is '**SOF basic**' (Strength of Functions Basic).

2. TOE Description

The TOE - DAI-Labor's Java Intelligent Agent Componentware IV - is comprised by a platform running on a Java Virtual Machine (version 1.4.2_04), which constitutes the runtime environment. The purpose of this runtime environment is to provide access to the host system resources and an interface between the local agent platform and the underlying OS. The local platform can be seen as an organisational unit offering infrastructural services to the platform itself, such as agent migration as well as application services to human users. All services whether they suite needs of an application, i.e. a public service, or are used to manage the internal infrastructure are provided and carried out by JIAC IV agents.

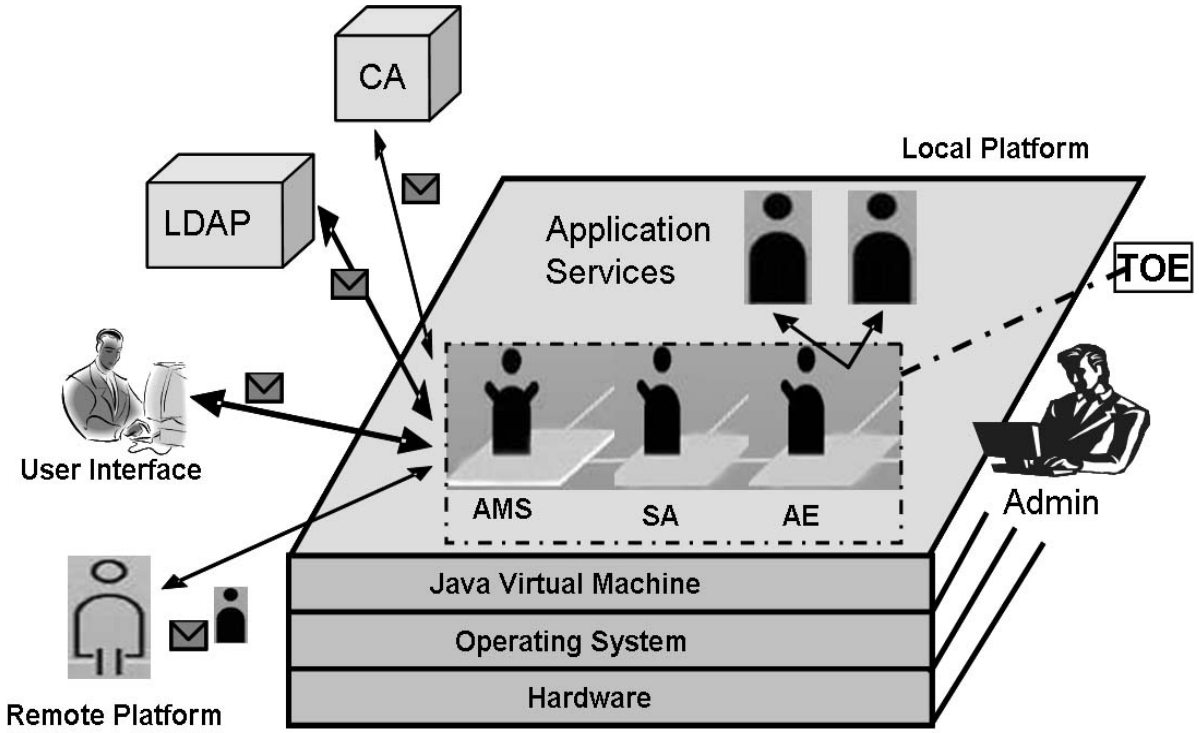

Figure 1: Basic Structure of the TOE and its Interaction with the Environment

Figure 1 illustrates the TOE that comprises the Agent Management System (AMS), the Security Agent (SA), and the Alter Ego (AE), which are (one and two arms) infrastructure agents as described in 2.1. As it can be seen any external communication is completely and solely handled by the AMS (two arms). Communication is given by speech-acts (envelopes) and mobile agent (no arms) transfer from and to the external entities (Certification Authority, LDAP, User Interface and Remote Platform). The communication between local platform residing agents can take place bidirectional. All platform agents are registered at the AMS.

Further more the figure displays the local platform and its physical scope or boundary that is embedded within a Java Virtual Machine acting as an interpreter between the implemented scenario in Java byte code and the computer's operating system. The agent platform is running on a server machine and has a connection to the Internet, so that its services are available over a wide area network. This computer is administrated by an Administrator who only has a direct physical access to configure the platform, add services, maintain rudimentary availability, and fulfil further service level agreements.

2.1. Separation between the Local Platform and the TOE

The “Target of Evaluation” (TOE), as in the meaning of Common Criteria, consists of the agents responsible for security functional behaviour as well as offering and maintaining the infrastructure of the local platform by stationary management agents. The TOE comprises the following basic set of 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 via the Agent Communication Channel (ACC).
- *SecurityAgent (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 RP and UI.
- *AlterEgo (AE):* The AE represents the missing link between a graphically User Interface, that resides remotely on a Navigator platform, and the application services registered on the local platform. The AE is responsible for interpretation of the given human user commands.

The testable configuration of the TOE comprises an e-Business scenario implemented by *Service Agents* acting on the platform which are not within the scope of the TOE. These Service Agents do not implement any security functionality and are therefore not part of the TOE but of its environment. The agents interact by use of services, guided by protocols. The service agent acting on behalf of a human user is an application service initiated by the AE which applies the parameters/requests given by the user interface. During agent creation each service gets registered at the Directory Facilitator, which is a part of the AMS, automatically.

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.

Intended e-Business scenarios are e.g. services to get or offer proposals (e.g. hotel reservations or flight schedules), trading transactions and communication for minor valued operations with a low requirement for protection (e.g. online ordering from a catalogue).

2.2. Platform communication levels and interfaces

Internally the platform (TOE) uses speech acts on behalf of the capabilities of the underlying Java Virtual Machine (JVM). The JVM exchanges internal messages between local agents to distribute their messages.

The Agent Management System (AMS) is the only instance on the agent platform which is able to establish a communication channel to remote systems to exchange Remote Platform data, using the Agent Communication Channel (ACC). A special case of data exchange is the mobile agent scenario between the local platform (that comprises the TOE) and a Remote Platform. To fulfil the requirements of knowing how service agents can be addressed the Directory Facilitator (DF) of the AMS communicates with a Lightweight Directory Access Protocol (LDAP) server that provides a yellow pages directory that covers service agents of all registered platforms.

In order to provide a basic level of trustworthiness, as interpreted and verified by the SecurityAgent, a Certification Authority (CA) is enrolled and maintained by a trusted third party. It shall provide Certificates over User Interfaces, and Remote Platforms to bear witness of their trustworthiness as well as a certificate revocation list, which can be understood as a blacklist of Certificates that are no longer classified as being trustworthy.

Finally the connection between the remote User Interface and the AlterEgo agent provides access to locally registered application services. This interface between the TOE and any human user can be represented as a single point of service by which the user can access the local platform comprising the TOE. Further more it is possible for local services to use application services residing on a Remote Platform as an extension to additional services.

2.3. Logical boundaries of the TOE

In the following the basic security functionalities that are implemented within the TOE are represented to clarify the security behaviour and environment of the TOE. The implemented functionalities of the TOE can be separated by the following categories: communication, crypto-support, user data protection, and security management.

2.3.1. Communication and trusted channels

External communication can be established either by a Secure Socket Layer (SSL/TLS) Protocol or by TCP/IP. All connections, coming from a User Interface, a Remote Platform, and a Certification Authority (CA) are established via a secure network connection[1]. This security feature restricts secure communication channels only to trustworthy entities so that intrusion of malicious agents or other executable applets can be prevented. The CA is responsible for signing and publishing valid certificates over trustworthy RP and UI. Further more the CA publishes the certificate revocation list to filter out platforms that are not considered as being trustworthy anymore.

On the other side data transmitted by an unsecured communication, i.e. TCP/IP are only accepted or send as LDAP-data which is used to provide or to ask for information about agents that offer application services and other available services on remote agent platforms.

2.3.2. Cryptographic support

Cryptographic mechanisms are limited to generation of asymmetric key-pairs, the possibility to encrypt and decrypt the communication channel by SSL based on the same key-pair, and signature verification of (CA) signed public keys and SHA-1 signed objects. Cryptographic

1 LDAP, RP, UI, and CA are explicitly not part of the TOE itself.

support is considered to be strong because RSA[2] is used with key-size of 1024 or 2048bit and connections to trustworthy entities share the same specifications for RSA key-sizes.

To avoid statistical weaknesses during the generation of (pseudo-) random numbers, used during establishment of an SSL/TLS communication channel and generation of asymmetrical key-pairs, the TOE comprises its own random number generator (PRNG). The PRNG is seeded with "non-deterministic" entropy that was generated along with activities by the Administrator of the local platform during the start-up procedure.

2.3.3. User data protection and identification & authentication

The communication access is controlled by the TOE to differentiate between data exchanged from the TOE to trustworthy RP and UI, the LDAP, and the CA. This assures that sensitive user data with security attributes are only exchanged between the TOE and the identified UI. Also the TOE is always able to interpret and relate imported user data with and without security attributes to the identified human user. Communication access also ensures the integrity of exchanged data by the underlying SSL/TLS connection on one side and by the verification of signed data (i.e. certificates and the certificate revocation list) on the other.

Every user interface is therefore verified by two ways, first by the CA-signed certificate during SSL/TLS connection and second by the TOE user identification & authentication process. TOE identification & authentication requires strong passwords and circumvents timing attacks.

2.3.4. Security management and protection of the security functions

Installation, generation, configuration, and usage of the platform that comprises the TOE (AMS, SA, AE) is limited only to the Administrator and is restricted to the following activities:

- Enable and disable external communication of the platform,
- Generate and delete the TOE asymmetrical key-pair,
- Import the public key of the Certification Authority,
- Create, delete, and modify user identification and authentication data, and
- Create, delete, and modify infrastructure- and service agents.

To assure that to entities such as RP, UI, and CA only an SSL/TLS connection is used, the TOE uses security attributes that are set according to successful signature verification.

Detected states of error can be grouped by the following three categories:

(i) Instantiation and lifecycle control of agents, i.e. wrong properties or missing crypto-components, instantiation of duplicate agents during registration at the AMS,

(ii) Communication and handling of speech act and mobile agent data via the agent communication channel in accordance to the specified format, and

(iii) Management of functionalities involved in crypto support, i.e. initiation of SSL connections, reading of local key-pair, certificates, and a certificate revocation list.

2 Crypto-algorithms (e.g. RSA, SHA-1, SSL/TLS) are restricted by specified TOE limitations and used by the IAIK library.

2.4. Physical boundary of the TOE

Public distribution of the TOE is realised by Web page access. The 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 needed java components (J2SDK version 1.4.2_04 and JCE version 1.4.2) can also be downloaded from this location but are not part of the TOE itself.

The physical boundary of the TOE delivery package (JIAC-IV_Cert_4_3_11.zip) can be separated by the following items:

- All Java archives that were developed by the DAI-Labor and that belong to the certification release[4] of JIAC IV (including Component Architecture, Knowledge Infrastructure, Ontology Compiler, Security Component, JIAC Utilities, Control for Knowledge Infrastructure and Component Architecture, Infrastructure Architecture, and the JIAC Interface to the IAIK libraries), as well as
- All Java archives that were used as third-party libraries (IAIK Cryptography Extensions version 3.0.3 and the iSaSiLk SSL Libraries version 3.0.6, and Netscape Directory SDK version 4.0) to realise specific functionality of the local platform, and finally the
- Administrator and user guidance, holding information on how to administer, install, configure and use the TOE.

For a more complete list of the TOE implementation representation (i.e. the components or subsystems that compose the TOE) and for explicitly defined version numbers the configuration list ([13]) is recommended.

4 For explicitly defined version numbers the configuration list ([13]) is recommended.

3. TOE security environment

Assets

The TOE is intended to be used for common communication transactions. For this, actions like collecting or purchasing information (i.e. flight schedules, booking hotel accommodation etc.) are executed. The TOE is not intended to handle high sensitive information or strictly confidential data (e.g. information concerning military or national security purpose).

Asset	Security Goal	Definition
User Data	Integrity and confidentiality	Speech-act comprising identification and authentication data, and user application data
Mobile Agent	Integrity and confidentiality	Speech-act containing mobile agent data (i.e. executable code) and mobile agent data (i.e. service application data)
CA Data	Integrity	Speech-act containing certificates and CRLs
RP Data	Integrity and confidentiality	Speech-act used for communication between agents on different trustworthy platforms.
TOE Private Key	Integrity and confidentiality	Private key data used for establishing SSL/TLS connections.
Platform Sustainability	Integrity	Only stationary agents residing at the TOE and mobile agents originated by trustworthy platforms are executed by the local platform (TOE). No TOE-residing agent circumvents the TSP.

Table 1: TOE Assets

Subjects

Subjects	Definition
User	Somebody having access to the platform via a trusted user interface and having the ability to initiate a service agent acting on his behalf. A user is verified by the TOE by an appropriate identification and authentication procedure.
Administrator	A user which has physical access to the platform and the ability to administer the TOE. An Administrator is verified by the underlying OS identification and authentication procedure, and needs to activate the TOE key-pair with a password (provided by the TOE). The direct access to the platform allows configuration of security critical functions. The Administrator is a reliable person and has to follow the guidance documentation as provided for the TOE.

Table 2: TOE Subjects

Application note: The Certification Authority (CA) provides certificates over trustworthy entities. Depending on the validity of these certificates some TOE internal attributes are set.

For this the CA is mentioned as an identified role in FMT_MSA.1 (section 5.1.5.2, p 7) and might also be seen as a subject.

Threat agents[5]

Threat agents	Definition
Net-Attacker	Somebody acting outside the platform with a malicious intention. An attacker has no direct access to any trustworthy platform, but is able to monitor data packages transferred via the shared network. The attacker has no specialised knowledge to perform the respective attack and has only public IT, OS and TOE knowledge. The attacker has no access to specialised or bespoke hacker equipment. For this the attacker is presumed to have an attack potential utilising obvious vulnerabilities only.

3.5. Assumptions

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.

3.6. Threats

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

5 The term "threat agent" is given by the CC and shall not be confused with the term agent as defined in the glossary.

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.

3.7. Organisational security policies

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.

4. Security Objectives

This section identifies and defines the security objectives for the TOE and its environment. Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

4.1. Security Objectives for the TOE

OT.Crypt: Usage of robust encryption and signing techniques

The TOE should use appropriate cryptographic methods to ensure that signatures cannot be forged and data encryption cannot be broken[6].

OT.Data_Receive: Reliability of received data

The TOE shall ensure that data not received from a trustworthy remote platform, trustworthy remote user interface, or a Certification Authority are only accepted as LDAP information.

OT.Data_Send: Confidentiality of send data

The TOE shall ensure that only LDAP data are sent over a not secured communication channel. Secured communication channels can only be established to trustworthy remote platforms, trustworthy remote user interfaces, or a Certification Authority.

OT.RP_Data_Receive: Speech act data received by a remote platform

The TOE shall only accept speech act and mobile agent data with a successfully checked confidentiality and integrity protection send by a trustworthy remote platform as speech act data or mobile agent data.

OT.RP_Data_Send: Speech act data send to a remote platform

The TOE shall ensure that the remote platform is able to check the authenticity and integrity of speech act and mobile agent data. The protection of the confidentiality shall ensure that these data are only accessible for the intended trustworthy remote platform.

OT.UI_Data_Receive: User application data received by a user interface

The TOE shall only accept data with a successfully checked confidentiality and integrity protection send by a trustworthy remote user interface (UI) as user application data.

OT.UI_Data_Send: User application data send to a user interface

The TOE shall ensure the ability to check the authenticity and integrity of sent user application data. The protection of the confidentiality shall ensure that these data are only accessible for the intended trustworthy remote user interface (UI).

OT.Trusted_CA: Spoofing of a trustworthy Certification Authority

The TOE shall ensure that certificates and the certificate revocation list are only accepted when they are generated from a trustworthy Certification Authority (CA) and when the data integrity was successfully verified.

4.2. Security objectives for the environment

OE.Restricted_Access: Physical and logical access to the TOE

6 This accomplishes that the private key cannot be derived by knowledge of the public key, the signature, or the encrypted data.

The TOE environment shall restrict the physical access to the TOE to authorised persons (S.Administrator) interacting with the platform and with the server (hardware and software) only. The direct physical access is the only way to administer the TOE.

Further more the IT-Environment (HW, OS) has to ensure the protection of the resources used by the TOE against external attacks.

OE.CA_Cert: Certificates and CRL as generated by the Certification Authority

The Certification Authority (CA) generates and provides reliable and unforgeable certificates based on strong cryptography over the following entities:

- trustworthy remote platforms and
- trustworthy user interfaces

The certificate shall include the entities identity, the date of validity and the public-key. The CA has to take appropriate measures to keep the list of certificates updated. Furthermore the CA provides the updated certificate revocation list (CRL) to ensure the up-to-dateness of the certificate data.

OE.RP_Trust: Trusted remote platform environment

A trusted remote platform solely sends speech act and mobile agent data. These data do not contain any malicious or illicit data.

OE.RP_Trans: Secure data transfer to and from the remote platform

The remote platform shall provide and use adequate mechanisms to ensure the confidentiality and integrity of data transferred between the TOE and itself.

OE.UI_Trust: Trusted remote user interface environment

The User Interface (UI) maintains the integrity and confidentiality of data for the identification and authentication of the human user and of the user application data within the User Interface.

OE.UI_Trans: Secure data transfer to and from the remote user interface

The user interface shall only send identification, authentication, and user application data to the platform. The UI shall provide and take adequate measures to ensure the confidentiality and integrity of those data during transfer from and to the TOE.

5. IT Security Requirements

This chapter defines the security functional requirements and the security assurance requirements for the TOE and its environment. The chapter is organised as follows. Section 5.1 “TOE Security Functional Requirements” gives security functional requirements; and following Section 5.2 “TOE Security Assurance Requirements“ defines security assurance requirements for the TOE. Security requirements for TOE IT and non-IT environments are given in the Section 5.3 and in Section 5.4, respectively.

The requirements given in section 5.1 and 5.3 are drawn from the Common Criteria, Part 2: Security functional requirements [2]. The requirements given in section 5.2 are drawn from the Common Criteria, Part 3: Security assurance requirements [3]. The requirements incorporate TOE-specific method and algorithms assignments.

5.1. TOE Security Functional Requirements

5.1.1. Communication (FCO)

5.1.1.1. Selective proof of origin (FCO_NRO.1)

Certification Authority data

FCO_NRO.1.1	The TSF shall be able to generate evidence of origin for transmitted certificates over remote platforms or user interfaces and the certificate revocation list[7] at the request of the recipient[8].
FCO_NRO.1.2	The TSF shall be able to relate the attributes: “certificate valid” and “actual CRL”[9] of the originator of the information, and the certificate’s and certificate revocation list’s body[10] of the information to which the evidence applies.
FCO_NRO.1.3	The TSF shall provide a capability to verify the evidence of origin of information to recipient[11] given indefinite limitations[12].

Application note: The recipient in FCO_NRO.1.1 is the TOE. The signatures being applied to the certificate and to the certificate revocation list (CRL) are checkable without any temporal limitation as given by the strength of the used cryptographic operation.

5.1.2. Cryptographic support (FCS)

5.1.2.1. Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm used for key

7 [assignment: list of information types]

8 [selection: originator, recipient, [assignment: list of third parties]]

9 [assignment: list of attributes]

10 [assignment: list of information fields]

11 [selection: originator, recipient, [assignment: list of third parties]]

12 [assignment: limitations on the evidence of origin]

	generation that was published in CryptoBytes Vol. 3, Number 1 [12][13] and specified cryptographic key sizes of 1024 or 2048 bit[14] that meet the following: ANSI X9.31 criteria for RSA key generation[15].

5.1.2.2. Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method zeroising of key data[16] that meets the following: none[17].

Application note: The private key has to be zeroised (overwritten), at least before the generation of a new key pair.

5.1.2.3. Cryptographic operation (FCS_COP.1)

FCS_COP.1.1 / SSL	The TSF shall perform encryption and decryption of transferred data[18] in accordance with a specified cryptographic algorithm cipher suits[19]: • SSL_RSA_WITH_3DES_EDE_CBC_SHA and cryptographic key size[20]: • SSL_RSA_WITH_3DES_EDE_CBC_SHA (RSA: of 1024 or 2048 bit, 3DES: 168 bit, SHA: none) that meet the following: SSLv3.0 / TLS 1.0.[21]

Application note: The SSL 3.0/TLS 1.0 cipher suite as specified above uses the cryptographic algorithms RSA, 3DES and SHA1. These algorithms are implemented by the IAIK JCE (version 3.0) and IAIK iSaSiLk Toolkit (version 3.0.5), which are crypto libraries and part of the TOE deliverables (see "Physical boundary of the TOE" in chapter 2.4).

FCS_COP.1.1 / sig_verify	The TSF shall perform signature verification[22] in accordance with a specified cryptographic algorithm RSA and SHA[23] and cryptographic key sizes of 1024 or 2048 bit (RSA) and none (SHA1)[24] that meet the following: PKCS #1: RSA Encryption Standardand FIPS PUB 180-1 (SHA1)[25].

13 [assignment: cryptographic key generation algorithm]
14 [assignment: cryptographic key sizes]
15 [assignment: list of standards]
16 [assignment: cryptographic key destruction method]
17 [assignment: list of standards]
18 [assignment: list of cryptographic operations]
19 [assignment: cryptographic algorithm]
20 [assignment: cryptographic key sizes]
21 [assignment: list of standards]
22 [assignment: list of cryptographic operations]
23 [assignment: cryptographic algorithm]
24 [assignment: cryptographic key sizes]
25 [assignment: list of standards]

5.1.3. User data protection (FDP)

5.1.3.1. Subset access control (FDP_ACC.1)

User, subject or object the attribute is associated with	Attribute	Status
General Attribute		
User	role	user interface, remote platform, LDAP, Certification Authority, none
Connection Attribute		
user interface, remote platform, LDAP	trusted SSL connect	no, yes
Data Attribute Group		
Certification Authority	valid certificate	no, yes
Certification Authority	actual CRL	no, yes

Table 3: Subset Access Control

User interface SFP

FDP_ACC.1.1 / UI	The TSF shall enforce the user interface SFP[26] on subject: user interface, objects: agent application data, send user application data for initiation of service agents to the TOE.[27]

User interface SFP

FDP_ACF.1.1 / UI	The TSF shall enforce the user interface SFP[28] to objects based on Connection attribute and General attribute[29].
FDP_ACF.1.2 / UI	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute “role” set to “user interface” and the user interface with the security attribute “trusted SSL connect” is set to “yes” is allowed to: 1. Send user application data for initiation of a service carried out by a service-agent to the TOE. 2. Receive user application data generated of service (-agent)

26 [assignment: access control SFP]

27 [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

28 [assignment: access control SFP]

29 [assignment: security attributes, named groups of security attributes]

	from the TOE.[30] 3. Send user identification and authentication data.
FDP_ACF.1.3 / UI	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[31].
FDP_ACF.1.4 / UI	The TSF shall explicitly deny access of subjects to objects based on the rules[32]: 1. The user with the security attribute role not set to "user interface" is not allowed to: a) Send user application data for initiation a service carried out by a service-agent to the TOE. b) Receive user application data generated by a service (-agent) from the TOE. c) Send user identification and authentication data. 2. The user with the security attribute role set to "user interface" and the user interface with the security attribute "trusted SSL connect" is set to "no" is not allowed to: a) Send user application data for initiation a service carried out by a service-agent to the TOE. b) Receive user application data generated by a service (-agent) from the TOE. c) Send user identification and authentication data.

Remote Platform SFP

FDP_ACC.1.1 / RP	The TSF shall enforce the remote platform SFP[33] on subject: remote platform, objects: speech act and mobile agent data, send or receive speech act or mobile agent data to / from the TOE[34].

Remote Platform SFP

FDP_ACF.1.1 / RP	The TSF shall enforce the remote platform SFP[35] to objects based on Connection attribute and General attribute[36].
FDP_ACF.1.2 / RP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is

30 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

31 [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

32 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

33 [assignment: access control SFP]

34 [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

35 [assignment: access control SFP]

36 [assignment: security attributes, named groups of security attributes]

	allowed: The user with the security attribute “role” set to “remote platform” and the remote platform with the security attribute “trusted SSL connect” is set to “yes” is allowed to: 1. Send mobile agent application data to the TOE, 2. Receive mobile agent application data from the TOE, 3. Send speech act data to the TOE and 4. Receive speech act data from the TOE[37].
FDP_ACF.1.3 / RP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[38].
FDP_ACF.1.4 / RP	The TSF shall explicitly deny access of subjects to objects based on the user with the security attribute “role” not set to “remote platform” or the remote platform with the security attribute “trusted SSL connect” is set to “no” is not allowed to: 1. Send mobile agent application data to the TOE, 2. Receive mobile agent application data from the TOE, 3. Send speech act data to the TOE and 4. Receive speech act data from the TOE[39].

LDAP SFP

FDP_ACC.1.1 / LDAP	The TSF shall enforce the LDAP SFP[40] on subject: LDAP, object: send or receive registration information about available agents/services to / from the TOE[41].

LDAP SFP

FDP_ACF.1.1 / LDAP	The TSF shall enforce the LDAP SFP[42] to objects based on Connection attribute and General attribute[43].
FDP_ACF.1.2 / LDAP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: 1. Data received over a connection with the security attribute

37 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

38 [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

39 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

40 [assignment: access control SFP]

41 [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

42 [assignment: access control SFP]

43 [assignment: security attributes, named groups of security attributes]

	"trusted SSL connect" is set to "no" are only accepted as agent registration information from an LDAP Server. 2. Only agent registration information provided for an LDAP shall be sent over a connection with the security attribute "trusted SSL connect" is set to "no"[44]
FDP_ACF.1.3 / LDAP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[45].
FDP_ACF.1.4 / LDAP	The TSF shall explicitly deny access of subjects to objects based on: 1. All Data received over a connection with the security attribute "trusted SSL connect" set to "no" are interpreted as agent registration information from an LDAP Server and rejected in case of mismatch. 2. No data shall be sent over a connection with the security attribute "trusted SSL connect" is set to "no" except agent registration information to an LDAP[46].

Certification Authority SFP

FDP_ACC.1.1 / CA	The TSF shall enforce the Certification Authority SFP[47] on subject: Certification Authority, object: send certificates and CRL to the TOE[48].

Certification Authority SFP

FDP_ACF.1.1 / CA	The TSF shall enforce the Certification Authority SFP[49] to objects based on Connection attribute and General attribute[50].
FDP_ACF.1.2 / CA	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: The user with the security attribute "role" set to "Certification Authority" and the Certification Authority with the security attribute "trusted SSL connect" is set to "yes" is allowed to send: 1. Certificates over trustworthy remote platforms to the TOE, 2. Certificates over trustworthy user interfaces to the TOE, and

44 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

45 [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

46 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

47 [assignment: access control SFP]

48 [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

49 [assignment: access control SFP]

50 [assignment: security attributes, named groups of security attributes]

	3. The certificate revocation list to the TOE[51].
FDP_ACF.1.3 / CA	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[52].
FDP_ACF.1.4 / CA	The TSF shall explicitly deny access of subjects to objects based on the user with the security attribute "role" not set to "Certification Authority" or Certification Authority with the security attribute "trusted SSL connect" is set to "no" is not allowed to send: 1. The certificate revocation list to the TOE.[53]

5.1.3.2. Export of user data without security attributes (FDP_ETC.1)

FDP_ETC.1.1	The TSF shall enforce the remote platform SFP, Certification Authority SFP and LDAP SFP[54] when exporting user data, controlled under the SFP(s), outside of the TSC.
FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.

Application note: The remote platform SFP is addressed by the means of speech-act transfer. This affects remote platform data as well as mobile agent data.

5.1.3.3. Export of user data with security attributes (FDP_ETC.2)

FDP_ETC.2.1 / RP	The TSF shall enforce the remote platform SFP[55] when exporting user data, controlled under the SFP(s), outside of the TSC.
FDP_ETC.2.2 / RP	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3 / RP	The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.
FDP_ETC.2.4 / RP	The TSF shall enforce the following rules when user data is exported from the TSC: the service-ID shall be exported within the mobile agent[56].

Application note: The remote platform SFP is addressed by the means of mobile agent transfer.

FDP_ETC.2.1 / UI	The TSF shall enforce the user interface SFP[57] when exporting user data, controlled under the SFP(s), outside of the TSC.

51 [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]

52 [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]

53 [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

54 [assignment: access control SFP(s) and/or information flow control SFP(s)]

55 [assignment: access control SFP(s) and/or information flow control SFP(s)]

56 [assignment: additional exportation control rules]

57 [assignment: access control SFP(s) and/or information flow control SFP(s)]

FDP_ETC.2.2 / UI	The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.3 / UI	The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.
FDP_ETC.2.4 / UI	The TSF shall enforce the following rules when user data is exported from the TSC: the identity of the human user (identification data)[58].

5.1.3.4. Import of user data without security attributes (FDP_ITC.1)

FDP_ITC.1.1	The TSF shall enforce the remote platform SFP and LDAP SFP[59] when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.1.2	The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.
FDP_ITC.1.3	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: none[60].

Application note: The remote platform SFP is address by the means of speech-act transmission only. This affects remote platform data as well as mobile agent data.

5.1.3.5. Import of user data with security attributes (FDP_ITC.2)

FDP_ITC.2.1 / RP	The TSF shall enforce the remote platform SFP[61] when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.2.2 / RP	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3 / RP	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4 / RP	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5 / RP	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: 1. Import and maintenance of the agent associated service-ID within the agent data[62].

58 [assignment: additional exportation control rules]

59 [assignment: access control SFP and/or information flow control SFP]

60 [assignment: additional importation control rules]

61 [assignment: access control SFP and/or information flow control SFP]

Application note: The remote platform SFP is address by the means of mobile agent transmission only. FDP_ITC.2.3 seems to be incomplete and is therefore interpreted as: ”The TSF shall ensure that the protocol used provides *the functionality* for the unambiguous association between the security attributes and the user data received”.

FDP_ITC.2.1 / CA	The TSF shall enforce the Certification Authority SFP[63] when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.2.2 / CA	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3 / CA	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4 / CA	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5 / CA	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: 1. Successful verification of the signature over the imported certificate revocation list and 2. Successful verification of the signature over the imported certificate[64].

FDP_ITC.2.1 / UI	The TSF shall enforce the user interface SFP[65] when importing user data, controlled under the SFP, from outside of the TSC.
FDP_ITC.2.2 / UI	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3 / UI	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4 / UI	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5 / UI	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: the identity and

62 [assignment: additional importation control rules]

63 [assignment: access control SFP and/or information flow control SFP]

64 [assignment: additional importation control rules]

65 [assignment: access control SFP and/or information flow control SFP]

	authenticity of the human user identification and authentication data[66].

5.1.3.6. Stored data integrity monitoring and action (FDP_SDI.2)

The following data persistently stored by TOE have the user data attribute "integrity checked persistent stored data":

FDP_SDI.2.1	The TSF shall monitor user data stored within the TSC for integrity errors[67] on all objects, based on the following attributes: CA public key and the platforms (TOEs) key-pair[68].
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall stop all external communications and cryptographic operations[69].

5.1.3.7. Data exchange integrity (FDP_UIT.1)

FDP_UIT.1.1	The TSF shall enforce the remote platform SFP, user interface SFP, and Certification Authority SFP[70] to be able to transmit and receive[71] user data in a manner protected from modification, deletion, insertion, and replay[72] errors.
FDP_UIT.1.2	The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion, and replay[73] has occurred.

5.1.4. Identification and authentication (FIA)

5.1.4.1. User attribute definition (FIA_ATD.1)

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: 1. Security attribute service-ID being associated to agents acting on the behalf of this user. 2. Security attribute “role” “user interface” 3. Security attribute “role” “human user”[74]

Application note: The maintenance of the service-ID is important to associate the agent to the user belonging to it during the whole life cycle of the agent.

66 [assignment: additional importation control rules]
67 [assignment: integrity errors]
68 [assignment: user data attributes]
69 [assignment: action to be taken]
70 [assignment: access control SFP(s) and/or information flow control SFP(s)]
71 [selection: transmit, receive]
72 [selection: modification, deletion, insertion, replay]
73 [selection: modification, deletion, insertion, replay]
74 [assignment: list of security attributes]

5.1.4.2. Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet at least 8 alphanumerical characters[75].

5.1.4.3. Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 / human	The TSF shall allow establishing a trusted channel to the UI[76] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 / human	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user

FIA_UAU.1.1 / entity	The TSF shall allow send and receive LDAP data[77] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 / entity	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note: The authentication process is carried out during the establishment of the SSL connection. The identity of the entity is interrelated to the public key due to provided certificates (RP and UI) or due to the fact that the public key is TOE internally stored (CA) and integrity protected. The SSL connect ensures that the entity is in possession of its own associated private key.

5.1.4.4. Timing of identification (FIA_UID.1)

FIA_UID.1.1 / human	The TSF shall allow establishing a trusted channel to the UI[78] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 / human	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1.1 / entity	The TSF shall allow send and receive LDAP data[79] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2 / entity	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

75 [assignment: a defined quality metric]
76 [assignment: list of TSF-mediated actions]
77 [assignment: list of TSF-mediated actions]
78 [assignment: list of TSF-mediated actions]
79 [assignment: list of TSF-mediated actions]

5.1.4.5. User-subject binding (FIA_USB.1)

FIA_USB.1.1	The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Application note: There are two subjects being associated to users: (1) the service acting on behalf of the user has a unique service-ID. This service-ID can be associated to a (human) user by the original platform (AE). (2) The identification and authentication (reference) data associated with the (human) user.

5.1.5. Security management (FMT)

5.1.5.1. Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 / external	The TSF shall restrict the ability to disable and enable[80] the functions external communication[81] to the Administrator[82].

FMT_MOF.1.1 / admin	The TSF shall restrict the ability to determine the behaviour of disable, enable, and modify the behaviour of[83] the functions executed by agents[84] to the Administrator[85].

FMT_MOF.1.1 / user	The TSF shall restrict the ability to determine the behaviour of, enable, and modify the behaviour of[86] the functions carried out by initiated services acting on the behalf of the user[87] to the user and the Administrator[88].

Application note: The (human) user is able to initiate a service-agent so that the service agent is acting on his behalf. The term “modify the behaviour of” is by the means of changing the user-accessible service parameters. The functionality itself of the service-agent can only be modified by the Administrator.

5.1.5.2. Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1	The TSF shall enforce the Remote platform SFP, User interface SFP, LDAP SFP, and Certification Authority SFP[89] to restrict the ability to modify[90] the security attributes ‘role” and “trusted SSL connect”[91] to the CA[92].

80 [selection: determine the behaviour of, disable, enable, modify the behaviour of]
81 [assignment: list of functions]
82 [assignment: the authorised identified roles]
83 [selection: determine the behaviour of, disable, enable, modify the behaviour of]
84 [assignment: list of functions]
85 [assignment: the authorised identified roles]
86 [selection: determine the behaviour of, disable, enable, modify the behaviour of]
87 [assignment: list of functions]
[88 assignment: the authorised identified roles]
89 [assignment: access control SFP, information flow control SFP]
90 [selection: change_default, query, modify, delete, [assignment: other operations]]
91 [assignment: list of security attributes]
92 [assignment: the authorised identified roles]

Application note: The security attributes “role” and “trusted SSL connect” are modified in connection with the establishment of a trusted SSL connect basing on the identified entity role given by the successful validation of the certificate provided by the CA. The “role” UI and RP are set in connection with confirmation by a valid certificate. The “role” CA is set and confirmed in connection with the internally stored CA’s public key.

5.1.5.3. Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1	The TSF shall ensure that only secure values are accepted for security attributes.

Application note: FMT_MSA.2 occurred as dependency from FCS_COP.1, FCS_CKM.1 and FCS_CKM.4 and addresses the key length used for SSL, for signature verification and for key generation (and destruction) of the platform.

5.1.5.4. Static attribute initialisation (FMT_MSA.3)

FMT_MSA.3.1	The TSF shall enforce the Remote platform SFP, User interface SFP, LDAP SFP and Certification Authority SFP[93] to provide restrictive[94] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the none[95] to specify alternative initial values to override the default values when an object or information is created.

Application note: The security attribute “trusted SSL connect” and “role” are automatically set to the default values “no” and “none” before establishing a connection.

5.1.5.5. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 / Auth	The TSF shall restrict the ability to modify[96] the internally stored user authentication data belonging[97] to the identified user[98].

FMT_MTD.1.1 / I&A	The TSF shall restrict the ability to create and delete[99] the user identification and authentication data[100] to the Administrator[101].

FMT_MTD.1.1 / key-pair	The TSF shall restrict the ability to create and delete[102] the platforms (TOE) key pair[103] to the Administrator[104].

93 [assignment: access control SFP, information flow control SFP]
94 [selection: restrictive, permissive, other property]
95 [assignment: the authorised identified roles]
96 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
97 [assignment: list of TSF data]
98 [assignment: the authorised identified roles]
99 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]
100 [assignment: list of TSF data]
101 [assignment: the authorised identified roles]
102 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

FMT_MTD.1.1 / CA-key	The TSF shall restrict the ability to import[105] the Certification Authority's public key[106] to the Administrator[107].

5.1.5.6. Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1	The TSF shall be capable of performing the following security management functions: 1. Setting the default values of the security attribute "trusted SSL connect" to "no" and "role" to "none" before a communication channel is established. 2. Verification of the trustworthiness of remote platforms and user interfaces by verification of associated certificates. 3. Creation and deletion of key-pair for the platform (TOE) by the Administrator. 4. Import of the Certification Authority's public key (Administrator). 5. Creation and deletion of user identification and authentication data (Administrator). 6. Modification of user authentication data (user). 7. Creation, modification and deletion of agents / services acting on the platform (Administrator). 8. Instantiation of service agents acting on behalf of a user (user).[108]

Application note: "Verification of trustworthiness" is done by the TOE through checking of a validation date and a signature applied to each certificate (X.509) as issued by an accepted Certification Authority. In this meaning trustworthy remote platforms and user interfaces will only be used and interfered with, if the certificate they provided is valid as in specified terms.

5.1.5.7. Security roles (FMT_SMR.1)

FMT_SMR.1.1	The TSF shall maintain the roles remote platform (RP), user interface (UI), Certification Authority (CA), (human) user and Administrator.[109]
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

Application note: The Administrator gets authenticated by the OS and when entering the password to access the private key of the platform's key-pair. Any other user, communicating with the TOE via a secure channel, gets identified and verified by the TOE itself exclusively.

103 [assignment: list of TSF data]

104 [assignment: the authorised identified roles]

105 [selection: change_default, query, modify, delete, clear, [assignment: other operations]]

106 [assignment: list of TSF data]

107 [assignment: the authorised identified roles]

108 [assignment: list of security management functions to be provided by the TSF]

109 [assignment: the authorised identified roles]

The roles remote platform, user interfaces and Certification Authority are associated with the technical users (entities)

5.1.6. Protection of the TSF (FPT)

5.1.6.1. Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: detection of error on which the management level cannot react with an appropriate error recovery.[110]

Application note: Detected states of error can be grouped by the following three categories: (1) instantiation and lifecycle control of agents such as wrong properties or missing crypto-components, instantiation of a duplicate agent, and registration at the local platform (at the AMS and DF services), (2) communication and handling of speech act and mobile agent data via the agent communication channel in accordance to the specified meta-protocol and its format, and (3) management of functionalities that are involved in cryptographical functions such as crypto support over all, correct initiation of SSL connections, reading of local key-pair operation, PKCS#12, certificates (X.509), and the certificate revocation list.

5.1.6.2. Inter-TSF basic TSF data consistency (FPT_TDC.1)

FPT_TDC.1.1 / signature	The TSF shall provide the capability to consistently interpret signatures[111] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2 / signature	The TSF shall use verification of signature[112] when interpreting the TSF data from another trusted IT product.

FPT_TDC.1.1 / I&A	The TSF shall provide the capability to consistently interpret user identification and authentication data[113] when shared between the TSF and another trusted IT product.
FPT_TDC.1.2 / I&A	The TSF shall use verification of I&A data with internally stored reference data[114] when interpreting the TSF data from another trusted IT product.

FPT_TDC.1.1 / service-ID	The TSF shall provide the capability to consistently interpret service-ID number of mobile agents originally generated on this platform[115] when shared between the TSF and another trusted IT

110 [assignment: list of types of failures in the TSF]

111 [assignment: list of TSFdata types]

112 [assignment: list of interpretation rules to be applied by the TSF]

113 [assignment: list of TSF data types]

114 [assignment: list of interpretation rules to be applied by the TSF]

115 [assignment: list of TSF data types]

	product.
FPT_TDC.1.2 / service-ID	The TSF shall use association rules between user and service-ID[116] when interpreting the TSF data from another trusted IT product.

5.1.7. Trusted path/channels (FTP)

5.1.7.1. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1	The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2	The TSF shall permit the TSF[117] to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for: 1. Data exchange between the TOE and a remote platform, 2. Data exchange between the TOE and the user interface, 3. Data exchange between the TOE and the Certification Authority.[118]

5.1.7.2. Trusted path (FTP_TRP.1)

FTP_TRP.1.1	The TSF shall provide a communication path between itself and remote[119] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.
FTP_TRP.1.2	The TSF shall permit remote users[120] to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for user identification and authentication and agent application data.[121]

116 [assignment: list of interpretation rules to be applied by the TSF]

117 [selection: the TSF, the remote trusted IT product]

118 [assignment: list of functions for which a trusted channel is required]

119 [selection: remote, local]

120 [selection: the TSF, local users, remote users]

121 [selection: initial user authentication, [assignment: other services for which trusted path is required]]

5.2. TOE Security Assurance Requirements

Assurance Class	Assurance Components
ACM	ACM_CAP.3, ACM_SCP.1
ADO	ADO_DEL.1, ADO_IGS.1
ADV	ADV_FSP.1, ADV_HLD.2, ADV_RCR.1
AGD	AGD_ADM.1, AGD_USR.1
ALC	ALC_DVS.1
ATE	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
AVA	AVA_MSU.1, AVA_SOF.1, AVA_VLA.1

Table 4: Assurance Requirements: EAL(3)

5.2.1. Configuration management (ACM)

5.2.1.1. Generation support and acceptance procedures (ACM_CAP.3)

ACM_CAP.3.1D	The developer shall provide a reference for the TOE.
ACM_CAP.3.2D	The developer shall use a CM system.
ACM_CAP.3.3D	The developer shall provide CM documentation.

ACM_CAP.3.1C	The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.3.2C	The TOE shall be labelled with its reference.
ACM_CAP.3.3C	The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.newC	The configuration list shall uniquely identify all configuration items that comprise the TOE.
ACM_CAP.3.4C	The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.5C	The CM documentation shall describe the method used to uniquely identify the configuration items.
ACM_CAP.3.6C	The CM system shall uniquely identify all configuration items.
ACM_CAP.3.7C	The CM plan shall describe how the CM system is used.
ACM_CAP.3.8C	The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.9C	The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10C	The CM system shall provide measures such that only authorised changes are made to the configuration items.

5.2.1.2. Problem tracking CM coverage (ACM_SCP.1)

ACM_SCP.1.1D	The developer shall provide a list of configuration items for the TOE.

ACM_SCP.1.1C	The list of configuration items shall include the following: implementation representation and the evaluation evidence required by the assurance components in the ST.

5.2.2. Delivery and operation (ADO)

5.2.2.1. Detection of modification (ADO_DEL.1)

ADO_DEL.1.1D	The developer shall document procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2D	The developer shall use the delivery procedures.

ADO_DEL.1.1C	The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

5.2.2.2. Installation, generation, and start-up procedures (ADO_IGS.1)

Changes due to FI 051:

ADO_IGS.1.1D	The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C	The installation, generation and start-up documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

5.2.3. Development (ADV)

5.2.3.1. Fully defined external interfaces (ADV_FSP.2)

ADV_FSP.1.1D	The developer shall provide a functional specification.

ADV_FSP.1.1C	The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2C	The functional specification shall be internally consistent.
ADV_FSP.1.3C	The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects,

	exceptions and error messages, as appropriate.
ADV_FSP.1.4C	The functional specification shall completely represent the TSF.

5.2.3.2. Security enforcing high-level design (ADV_HLD.2)

ADV_HLD.2.1D	The developer shall provide the high level design of the TSF.

ADV_HLD.2.1C	The presentation of the high-level design shall be informal.
ADV_HLD.2.2C	The high-level design shall be internally consistent.
ADV_HLD.2.3C	The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.2.4C	The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.2.5C	The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.2.6C	The high-level design shall identify all interfaces to the subsystems of the TSF.
ADV_HLD.2.7C	The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.
ADV_HLD.2.8C	The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.
ADV_HLD.2.9C	The high-level design shall describe the separation of the TOE into TSP enforcing and other subsystems.

5.2.3.3. Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1D	The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C	For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

5.2.4. Guidance documents (AGD)

5.2.4.1. Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1D	The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C	The administrator guidance shall describe the administrative functions and interfaces available to the Administrator of the TOE.
AGD_ADM.1.2C	The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3C	The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4C	The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.
AGD_ADM.1.5C	The administrator guidance shall describe all security parameters under the control of the Administrator, indicating secure values as appropriate.
AGD_ADM.1.6C	The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.7C	The administrator guidance shall be consistent with all other documentation supplied for evaluation.
AGD_ADM.1.8C	The administrator guidance shall describe all security requirements for the IT environment that are relevant to the Administrator.

5.2.4.2. User guidance (AGD_USR.1)

AGD_USR.1.1D	The developer shall provide user guidance.

AGD_USR.1.1C	The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C	The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C	The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C	The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.
AGD_USR.1.5C	The user guidance shall be consistent with all other documentation supplied for evaluation.
AGD_USR.1.6C	The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5. Life cycle support (ALC)

5.2.5.3. Identification of security measures (ALC_DVS.1)

ALC_DVS.1.1D	The developer shall produce development security documentation.

ALC_DVS.1.1C	The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2C	The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

5.2.6. Tests (ATE)

5.2.6.1. Analysis of coverage (ATE_COV.2)

ATE_COV.2.1D	The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C	The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2C	The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

5.2.6.2. Testing: high-level design (ATE_DPT.1)

ATE_DPT.1.1D	The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C	The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

5.2.6.3. Functional testing (ATE_FUN.1)

ATE_FUN.1.1D	The developer shall test the TSF and document the results.
ATE_FUN.1.2D	The developer shall provide test documentation.

ATE_FUN.1.1C	The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C	The test plans shall identify the security functions to be tested and

	describe the goal of the tests to be performed.
ATE_FUN.1.3C	The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C	The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C	The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

5.2.6.4. Independent testing - sample (ATE_IND.2)

ATE_IND.2.1D	The developer shall provide the TOE for testing.
ATE_IND.2.1C	The TOE shall be suitable for testing.
ATE_IND.2.2C	The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

5.2.7. Vulnerability assessment (AVA)

5.2.7.1. Analysis and testing for insecure states (AVA_MSU.1)

AVA_MSU.1.1D	The developer shall provide guidance documentation.

AVA_MSU.1.1C	The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AVA_MSU.1.2C	The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.1.3C	The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.1.4C	The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

5.2.7.2. Strength of TOE security function evaluation (AVA_SOF.1)

AVA_SOF.1.1D	The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C	For each mechanism with a strength of TOE security function

	claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2C	For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

5.2.7.3. Highly resistant (AVA_VLA.1)

AVA_VLA.1.1D	The developer shall perform a vulnerability analysis.
AVA_VLA.1.2D	The developer shall provide vulnerability analysis documentation.

AVA_VLA.1.1C	The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2C	The vulnerability analysis documentation shall describe the disposition of obvious vulnerabilities.
AVA_VLA.1.3C	The vulnerability analysis documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

5.3. Security requirements for the IT environment

In the following SFR for the IT environment the term “TSF” is substituted by the term “IT environment” as a refinement given by final interpretation RI # 58.

5.3.1. Cryptographic Support (FCS)

5.3.1.1. Cryptographic operation (FCS_COP.1)

User Interface

FCS_COP.1.1 / E-SSL	The IT environment shall perform encryption and decryption of transferred data[122] in accordance with a specified cryptographic algorithm cipher suits[123]: • SSL_RSA_WITH_3DES_EDE_CBC_SHA and cryptographic key size: • SSL_RSA_WITH_3DES_EDE_CBC_SHA (RSA: 1024 or 2048 bit, 3DES: 168 bit, SHA: none)[124] that meet the following: SSLv3.0 / TLS 1.0[125].

122 [assignment: list of cryptographic operations]

123 [assignment: cryptographic algorithm]

124 [assignment: cryptographic key sizes]

Application note: IT environment is represented by the technical users “User interface”, “Remote platform” and “Certification Authority”. This builds the environmental pendant to 5.1.2.3 (see also FTP_ITC.1 / E).

FCS_COP.1.1 / E-sign	The IT environment shall perform signature generation over certificates and CRL[126] in accordance with a specified cryptographic algorithm RSA and SHA[127] and cryptographic key sizes of 1024 or 2048 bit (RSA) and none (SHA1)[128] that meet the following: PKCS #1: RSA Encryption Standard and FIPS PUB 180-1 (SHA1)[129].

5.3.2. User Interface (UI) Application

5.3.2.1. Selective proof of origin (FCO_NRO.1)

Certification Authority data

FCO_NRO.1.1 / E-CA	The IT environment shall be able to generate evidence of origin for transmitted Certification Authority (CA) data[130] at the request of the recipient[131].
FCO_NRO.1.2 / E-CA	The IT environment shall be able to relate the identity[132] of the originator of the information, and the certificate and certificate revocation list (CRL)[133] of the information to which the evidence applies.
FCO_NRO.1.3 / E-CA	The IT environment shall provide a capability to verify the evidence of origin of information to recipient[134] given indefinite limitations[135].

Application note: The recipient in FCO_NRO.1.1 / E-CA is the TOE. The CA generates signatures over certificates and the CRLs provided by this CA. The TOE is able to check this signature. This is the environmental pendant to 5.1.1.1.

5.3.3. Trusted path/channels (FTP)

5.3.3.1. Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1 / E	The IT environment shall provide a communication channel between itself and a remote trusted IT product that is logically

125 [assignment: list of standards]
126 [assignment: list of cryptographic operations]
127 [assignment: cryptographic algorithm]
128 [assignment: cryptographic key sizes]
129 [assignment: list of standards]
130 [assignment: list of information types]
131 [selection: originator, recipient, [assignment: list of third parties]]
132 [assignment: list of attributes]
133 [assignment: list of information fields]
134 [selection: originator, recipient, [assignment: list of third parties]]
135 [assignment: limitations on the evidence of origin]

	distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2 / E	The IT environment shall permit the TSF[136] to initiate communication via the trusted channel.
FTP_ITC.1.3 / E	The IT environment shall initiate communication via the trusted channel for: 1. Data exchange between the TOE and a remote platform, 2. Data exchange between the TOE and the user interface, 3. Data exchange between the TOE and the Certification Authority.[137]

5.4. Security Requirements for the Non-IT Environment

R.Restricted_Access

The TOE environment shall restrict the physical and logical access to the TOE for unauthorised persons. For this the person physically interacting with the platform and with the server (hardware and software) has to be understood as S.Administrator. The direct physical access is the only way to administer the TOE.

Further more the IT-Environment (HW, OS) has to ensure the protection of the resources used by the TOE against external attacks.

R.CA_Key_Management

The Certification Authority has to provide adequate organisational methods for key distribution/import. For this a platform Administrator has to submit the platform's public key during the registration procedure in a secure (integrity protected) manner (e.g. verification of a fingerprint, etc.). Also the Certification Authority's public key has to be transmitted to the platform in a way its integrity can be proven. Because there is no root certificate provided for the CA's public key which integrity can be proven.

R.CA_Certificate

The CA generates and provides reliable and unforgeable certificates over trustworthy platforms and user interfaces. The certificate shall include the entities identity, the date of validity and the public-key.

The CA has to take appropriate measures to keep the list of certificates updated. Furthermore the CA provides the updated certificate revocation list (CRL) to ensure the up-to-dateness of the certificate data.

R.RP_Management

A trustworthy remote platform solely sends speech act and mobile agent data. These data do not contain any malicious or illicit data.

136 [selection: the TSF, the remote trusted IT product]

137 [assignment: list of functions for which a trusted channel is required]

The remote platform has to be registered at the Certification Authority to provide a certificate over the corresponding public key for trustworthiness.

R.UI_Management

The trustworthy user interface has to maintain the integrity and confidentiality of data for the identification and authentication of the human user and of the user application.

The integrity of the user interface application has to be maintained. Furthermore the interface has to be registered at the Certification Authority to provide a certificate over the corresponding public key for trustworthiness.

The user identification and authentication data has to be submitted to the human user after registration at the platform. This procedure has to provide adequate organisational measures to ensure the integrity and confidentiality of the user identification and authentication data.

R.Service_Agents

Service agents acting on the platform shall neither be able to establish external communication, nor implement any functionality that conflicts or bypasses the TOE security functions. The S.Administrator has to ensure that only these types of service agents are implemented.

6. TOE Summary Specification

The TOE summary specification defines the instantiation of the security requirements for the TOE. The specification gives a description of all security functions (SF) and assurance measures of the TOE that meet the TOE security requirements.

6.1. TOE Security Functions

In order to meet the requirements, the TOE enforces the following five security functions:

SF1 User communication,

SF2 Remote platform Speech-act transmission,

SF3 LDAP based data exchange

SF4 Mobile agent transmission, and

SF5 Certificate and key management

The security functions SF1 to SF5 are subdivided into sub-functions to support a classical comprehension of classification of security functions. A TSFR mapping to the security functions SF1 to SF5 is shown in 8.5.1 an additional TSFR mapping to the sub-functions is provided in 8.5.2.

Each of the TOE security functions is described in the following sections in detail.

6.1.1. SF1 User communication

The TOE “SF1 User communication” establishes a secure communication channel between the TOE and a trustworthy remote user interface. This communication channel is used for the exchange of identification and authentication and user application data. The user application data are information used for the initiation of a service carried out by service-agents acting on the behalf of a human user or information describing the results of the service agent that is associated to the authenticated user.

The trustworthiness of the remote user interface is ensured by a certificate. The certificate proofs the authenticity of the remote user interface and the human user is authenticated on his given identification and authentication data. The validity and up-to-dateness of the certificate has to be successfully checked by the TOE (SF5) before a SSL connection is established.

SSL connection

The TOE ensures the communication by using the SSL protocol according to SSLv3.0/TLS1.0 with the cipher suit SSL_RSA_WITH_3DES_EDE_CBC_SHA and the following key length of RSA: 1024 or 2048 bit, 3DES: 168bit, SHA: none (FCS_COP.1/SSL). Accepting only secure values for the security attributes implies that the required key length is met (FMT_MSA.2).

The SSL protocol based on valid certificates for both connection sides provides the assured identification of both end points. This ensures protection of the integrity and confidentiality of the transmitted data and is thus to be seen as a trusted channel (FTP_ITC.1). The SSL provides also mechanisms to detect data manipulation and therefore protects the data from modification, deletion, insertion, and replay (FDP_UIT.1).

Entity Identification and Authentication

The user interface (UI) identifies itself at the TOE and will be authenticated after establishing the SSL and thus after successful validation of its certificate. The certificate can be send from the UI or is received from the CA (FIA_UAU.1/entity and FIA_UID.1/entity).

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 (FMT_MSA.3 and FMT_SMF.1, esp. point 1). The values of these attributes are set automatically in dependency on the successful establishment of a SSL connection ("trusted SSL connect" set to "yes") based on a successful verification of the entity ("role" set to "user interface") certificate provided by the CA (FMT_MSA.1 and FMT_SMF.1, esp. point 2).

Access Control

The TOE accepts data as user application data and identification and authentication data only when they are send over a SSL connection ("trusted SSL connect" set to "yes") from a trustworthy user interface ("role" set to "user interface") ensuring the integrity and confidentiality of these data. On the other side the TOE only sends user application data over a SSL connection to a trustworthy user interface (FDP_ACC.1/UI and FDP_ACF.1/UI). Further more the TOE maintains identification and authentication data that belongs to multiple human users so that the TOE can separate them.

The TOE receives identification and authentication data of the human (FIA_ATD.1, FDP_ITC.2/UI, and FMT_SMR.1). The secure communication between the (human) user and the trusted remote user interface facilitates the functionality to be used as a trusted path which protects the identification and authentication data from the human user transmitted to the TOE (FTP_TRP.1).

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 and can be sent to the trustworthy remote user interface that provides the trusted path to the human user currently being identified and authenticated (FIA_ATD.1; FDP_ETC.2/UI; FMT_SMR.1).

Human Identification and Authentication

The TOE identifies and authenticates the (human) user directly after establishing the SSL connection to the trustworthy user interface (FIA_UAU.1/human and FIA_UID.1/human). The TOE relates the role "user" to the received identification and authentication data and associates the transmitted data to the TOE after a successful identification and authentication process to the respective human user (FMT_SMR.1). The TOE provides a mechanism to verify pass-phrases (authentication data) with a minimal length of eight alphanumerical characters (FIA_SOS.1).

After the TOE received the complete user application data which are directly associated with the human user's identification and authentication data (FPT_TDC.1/I&A) the service agent will be initiated so that the service-agent is acting on behalf of the human user.

This agent gets a unique and definite service-ID to allow the TOE the association of the authenticated human user with this agent (FIA_USB.1 and FMT_SMR.1). The TOE is able to resolve and associate service IDs to identified and authenticated human users, when the service ID has been initiated by a service agent that belongs to the platform on which the TOE resides (FIA_ATD.1 and FMT_SMF.1, esp. point 8). Further more the service-ID is

maintained and can be related to an identified and authenticated user when the service agent migrated to a remote platform and returned to the TOE (FPT_TDC.1/I&A and FPT_TDC.1/service-ID).

Acting of the service agent is affected by a change of the user-accessible service parameters, as illustrated in the user visible interface (FMT_MOF.1/user and FMT_SMF.1, esp. point 8).

The TOE allows the Administrator to create and delete (human) user accounts (roles) by entering and deleting identification and authentication data associated with this role (FMT_MTD.1/I&A and FMT_SMF.1, esp. point 5). The TOE supports entering the authentication data consisting of alphanumerical characters with a minimal length of eight by an administrator interface (FIA_SOS.1). Once the Administrator created a user account the user has to activate his account by verifying the pass-phrase created by the Administrator and defining a new one, to keep the authentication data under the sole control of the user. The TOE allows an identified and authenticated user to modify his password anytime he wants to (FMT_MTD.1/Auth and FMT_SMF.1, esp. point 6).

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 (FPT_FLS.1). Only the Administrator of the TOE is allowed to enable and disable its external communication (FMT_MOF.1/external). Further more the TOE restricts the ability to disable, enable or determine and modify the behaviour of functions executed by agents to the Administrator (FMT_MOF.1/admin and FMT_SMF.1, esp. point 7).

6.1.2. SF2 Remote platform Speech-act transmission

The TOE "SF2 Remote platform Speech-act transmission" establishes a secure speech-act transmission to a trustworthy remote platform. In the following description speech-acts are exclusively interpreted as remote platform data.

The trustworthiness of the remote platform is ensured by a certificate. The certificate proofs the authenticity of the public key of the remote platform (setting "role" to "remote platform"). The validity and up-to-dateness of the certificate has to be successfully checked by the TOE (SF5) before a SSL connection is established (setting "trusted SSL connect" to "yes").

SSL connection

The TOE ensures the communication by using the SSL protocol according to SSLv3.0/TLS1.0 with the cipher suit SSL_RSA_WITH_3DES_EDE_CBC_SHA and the following key length of RSA: 1024 or 2048 bit, 3DES: 168bit, SHA: none (FCS_COP.1/SSL). Accepting only secure values for the security attributes implies that the required key length is met (FMT_MSA.2).

The SSL protocol based on valid certificates for both connection sides provides the assured identification of both end points. This ensures protection of the integrity and confidentiality of the transmitted speech-act data and is thus to be seen as a trusted channel (FTP_ITC.1). The SSL provides also mechanisms to detect data manipulation and therefore protects the data from modification, deletion, insertion, and replay (FDP_UIT.1).

Entity Identification and Authentication

The remote platform (RP) identifies itself at the TOE and will be authenticated after establishing the SSL and thus after successful validation of its certificate. The certificate can be send from the RP or is received from the CA (FIA_UAU.1/entity and FIA_UID.1/entity).

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 (FMT_MSA.3 and FMT_SMF.1, esp. point 1). The values of these attributes are set automatically in dependency on the successful establishment of a SSL connection (setting “trusted SSL connect” to “yes”) based on a successful verification of the entity (“role” set to “remote platform”) certificate provided by the CA (FMT_MSA.1 and FMT_SMF.1, esp. point 2).

Access Control

The TOE accepts data as speech-act data only when they are send over a SSL connection (“trusted SSL connect” set to “yes”) from a trustworthy remote platform (“role” set to “remote platform”) ensuring the integrity and confidentiality of these data as well as the TOE only sends speech-act data over a SSL connection to a trustworthy remote platform (FDP_ACC.1/RP and FDP_ACF.1/RP).

The speech-act data are sent and received only without security attributes (FDP_ETC.1 and FDP_ITC.1).

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 (FPT_FLS.1). Only the Administrator of the TOE is allowed to enable and disable its external communication (FMT_MOF.1/external). Further more the TOE restricts the ability to disable, enable or determine and modify the behaviour of functions executed by agents to the Administrator (FMT_MOF.1/admin and FMT_SMF.1, esp. point 7).

6.1.3. SF3 LDAP based data exchange

The ”SF3 LDAP based data exchange“ allows the exchange of address-information about registered agents on known platforms.

Access Control

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 then LDAP data that are agent registration information of (remote) 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 (FDP_ACC.1/LDAP and FDP_ACF.1/LDAP).

The data are imported and exported without any associated security attributes (FDP_ETC.1 and FDP_ITC.1).

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 (FMT_MSA.3, FMT_SMF.1, esp. point 1). The values of these attributes are set automatically in dependency on the successful establishment of a SSL connection (“trusted SSL connect” remains set to “no”) based on a successful verification of the certificate provided by the CA (FMT_MSA.1). 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.

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 (FPT_FLS.1). Only the Administrator of the TOE is allowed to enable and disable its external communication (FMT_MOF.1/external). Further more the TOE restricts the ability to disable, enable or determine and modify the behaviour of functions executed by agents to the Administrator (FMT_MOF.1/admin and FMT_SMF.1, esp. point 7).

6.1.4. SF4 Mobile agent transmission

The TOE “SF4 Mobile agent transmission” ensures a secure transmission of mobile agents between the TOE and a trustworthy remote platform. In the following description speech-acts are exclusively interpreted as mobile agent data.

The trustworthiness of the remote platform is ensured by a certificate. The certificate proofs the authenticity of the remote platforms public key (setting “role” to “remote platform”). The validity and up-to-dateness of the certificate has to be successfully checked by the TOE (SF5) before a SSL connection is established (setting “trusted SSL connect” to “yes”).

SSL connection

The TOE ensures the communication by using the SSL protocol according to SSLv3.0/TLS1.0 with the cipher suit SSL_RSA_WITH_3DES_EDE_CBC_SHA and the following key length of RSA: 1024 or 2048 bit, 3DES: 168bit, SHA: none (FCS_COP.1/SSL). Accepting only secure values for the security attributes implies that the required key length is met (FMT_MSA.2).

The SSL protocol based on valid certificates for both connection sides provides the assured identification of both end points. This ensures protection of the integrity and confidentiality of the transmitted mobile agent data and is thus to be seen as a trusted channel (FTP_ITC.1). The SSL provides also mechanisms to detect data manipulation and therefore protects the data from modification, deletion, insertion, and replay (FDP_UIT.1).

Entity Identification and Authentication

The remote platform (RP) identifies itself at the TOE and will be authenticated after establishing the SSL and thus after successful validation of its certificate. The certificate can be send from the RP or is received from the CA (FIA_UAU.1/entity and FIA_UID.1/entity).

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 (FMT_MSA.3 and FMT_SMF.1, esp. point 1). The values of these attributes are set automatically in dependency on the successful

establishment of a SSL connection ("trusted SSL connect" set to "yes") based on a successful verification of the entity ("role" set to "remote platform") certificate provided by the CA (FMT_MSA.1 and FMT_SMF.1, esp. point 2).

Access Control

The TOE accepts data as mobile agent data only when they are send over a SSL connection ("trusted SSL connect" set to "yes") from a trustworthy remote platform ("role" set to "remote platform") ensuring the integrity and confidentiality of these data as well as the TOE only sends mobile agent data over a SSL connection to a trustworthy remote platform (FDP_ACC.1/RP and FDP_ACF.1/RP).

The mobile agent data is sent and received with the security attribute service-ID as specified in (FDP_ETC.2/RP and FDP_ITC.2/RP).

The service-ID will always be maintained and transmitted within the mobile agent data. In case that the imported mobile agent was originally generated on the local platform (i.e. the TOE) the TOE resolves and associates the service-ID with the related (human) user who originated and initiated that service (FPT_TDC.1/service-ID). This requires that the (human) user who initiated the service is successfully identified and authenticated using the platform internally stored identification and authentication data (FIA_ATD.1).

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 (FPT_FLS.1). Only the Administrator of the TOE is allowed to enable and disable its external communication (FMT_MOF.1/external). Further more the TOE restricts the ability to disable, enable or determine and modify the behaviour of functions executed by agents to the Administrator (FMT_MOF.1/admin and FMT_SMF.1, esp. point 7).

6.1.5. SF5 Certificate and key management

"SF5 Certificate and key management" ensures the trustworthiness of a (trustworthy) entity. The TOE (local platform) provides the possibility to download certificates and a current certificate revocation list (CRL) from a Certification Authority (CA), before any SSL connection to a remote platform or to a remote user interfaces takes place.

SSL connection

The prevention of disclosure and modification of the certificates and certificate revocation list during transmission from the CA is secured by using a trusted channel (FTP_ITC.1) established by the mandatory usage of the SSL protocol according to SSLv3.0/TLS1.0 with the cipher suit SSL_RSA_WITH_3DES_EDE_CBC_SHA and the following key length of RSA: 1024 or 2048 bit, 3DES: 168bit, SHA: none (FCS_COP.1/SSL) with assured identification of both end points. Accepting only secure values for the security attributes implies that the required key length is met (FMT_MSA.2).

The SSL provides also mechanisms to detect data manipulation and thus protects the data from modification, deletion, insertion, and replay (FDP_UIT.1).

Entity Identification and Authentication

The Certification Authority (CA) identifies itself at the TOE and will be authenticated after successful establishment of the SSL connection. The CA's public key is internally stored on the local platform (FIA_UAU.1/entity and FIA_UID.1/entity)

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 (FMT_MSA.3 and FMT_SMF.1, esp. point 1). The values of these attributes are set automatically in dependency on the successful establishment of a SSL connection (setting "trusted SSL connect" to "yes") based on a successful verification of the entity (setting "role" to "Certification Authority") using the CA's public key internally stored in the TOE (FMT_MSA.1 and FMT_SMF.1, esp. point 2).

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 internal stored keys and switches to a secure state (i.e. stopping of all external communications) in case a integrity error was detected (FDP_SDI.2).

The TOE key-pair (especially the private key) can only be created and deleted by the Administrator (FMT_MTD.1/key-pair and FMT_SMF.1, esp. point 3). 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 published in [12] (FCS_CKM.1). The TOE provides also mechanisms to destroy the local platforms key-pairs by zeroisation (FCS_CKM.4). The CA's public-key can only be imported and stored by the Administrator (FMT_MTD.1/CA-key and FMT_SMF.1, esp. point 4).

Access Control

The trustworthy CA is allowed to transmit certificates and CRLs over the SSL secured connection. The TOE accepts CRLs only when they are received from a trustworthy CA transmitted over a SSL secured connection (FDP_ACC.1/CA and FDP_ACF.1/CA, requires FMT_SMF.1, esp. point 4).

Data being exported to a CA are without any associated security attributes (FDP_ETC.1). The TOE imports certificates and the certificate revocation list (CRL), which are signed by the Certification Authority (FDP_ITC.2/CA).

Verification of Signature

The signatures of the Certification Authority over the certificates and the certificate revocation list (CRL) are checked by the TOE (FPT_TDC.1/signature).

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 (FCO_NRO.1). 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 (FCS_COP.1/sig_verify) ensuring that the CA is the originator (FCO_NRO.1). 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.

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 (FPT_FLS.1). Only the Administrator of the TOE is allowed to enable and disable its external communication (FMT_MOF.1/external). Further more the TOE restricts the ability to disable, enable or determine and modify the behaviour of functions executed by agents to the Administrator (FMT_MOF.1/admin and FMT_SMF.1, esp. point 7).

6.2. Assurance measures

TOE implements the assurance measures exactly drawn from the assurance requirements defined in sec. 5.2. Naming of each assurance measure is derived from the name of the according assurance requirement.

The TOE implements the following assurance measures by providing the appropriate documents and activities:

Assurance Measures	Remarks
ACM_CAP.3M	configuration management documentation
ACM_SCP.1M	configuration management documentation
ADO_DEL.1M	parts of delivery documentation
ADO_IGS.1M	secure installation, generation and start-up procedures
ADV_FSP.1M	fully defined external interfaces
ADV_HLD.2M	high-level design (security enforcing)
ADV_RCR.1M	correspondence analysis between TOE summary specification and fully defined external interfaces, functional specification and high-level design,
AGD_ADM.1M	administrator guidance
AGD_USR.1M	user guidance
ALC_DVS.1M	development security documentation
ATE_COV.2M	test coverage analysis
ATE_DPT.1M	depth of testing analysis
ATE_FUN.1M	test documentation
ATE_IND.2M	the TOE suitable for testing
AVA_MSU.1M	administrator and user guidance, misuse analysis
AVA_SOF.1M	strength of function claims analysis
AVA_VLA.1M	vulnerability assessment

Table 5: TOE Assurance Measures

7. PP claims

7.1. PP reference

The ST is not compliant to any PP.

7.2. PP refinements

The ST is not compliant to any PP. For this no PP refinements are made.

7.3. PP additions

The ST is not compliant to any PP. For this no PP additions are made.

8. Rationale

8.1. Security objectives rationale

8.1.1. Security Objectives Coverage

Threats – Assumptions - Policies / Security objectives	OT.Crypt	OT.Data_Receive	OT.Data_Send	OT.RP_Data_Receive	OT.RP_Data_Send	OT.UI_Data_Receive	OT.UI_Data_Send	OT.Trusted_CA	OE.Restricted_Access	OE.CA_Cert	OE.RP_Trust	OE.RP_Trans	OE.UI_Trust	OE.UI_Trans
A.CA_Cert										X				
A.User_Interface													X	X
A.Remote_Platform											X			
A.Access									X					
T.RP_Data	X			X	X							X		
T.Mobile_Agent	X			X	X							X		
T.User_Data	X					X	X							
T.CA_Data	X							X		X				
P.RP_Communication				X	X					X				
P.UI_Communication						X	X			X				
P.LDAP_Communication		X	X											
P.CA_Communication								X						

Table 6: Security Environment to Security Objectives Mapping

8.1.2. Security Objectives Sufficiency

8.1.2.1. Policies and Security Objective Sufficiency

P.RP_Communication (Communication with trustworthy platforms) is addressed by OT.RP_Data_Receive and OT.RP_Data_Send which ensure, that remote platform data and mobile agent data are only send to and received from trustworthy remote platforms. The trustworthiness is ensured by the certificates and the certificate revocation list provided by OE.CA_Cert.

P.UI_Communication (Communication with trustworthy user interfaces) is addressed by OT.UI_Data_Receive and OT.UI_Data_Send which ensure, that user identification and authentication data, and user application data are only send to and received from trustworthy user interfaces. The trustworthiness is ensured by the certificates and the certificate revocation list provided by OE.CA_Cert.

P.LDAP_Communication (Communication with LDAP) is addressed by OT.Data_Receive and OT.Data_Send which ensure, that plain text (agent registration information) is only send to and received from the LDAP server.

P.CA_Communication (Communication with Certification Authority) is addressed by OT.Trusted_CA which ensures that certificates and the certificate revocation list are only accepted when they are generated by a trustworthy Certification Authority of which the TOE has verified the signature and the integrity of the received data.

8.1.2.2. Threats and Security Objective Sufficiency

T.RP_Data (Modification or eavesdropping of communication data during transfer) is encountered by OT.RP_Data_Receive which ensures that remote platform data is only accepted from a trustworthy remote platform after a successful verification of integrity and confidentiality. On the other side OT.RP_Data_Send ensures that remote platform data will only be send to the intended trustworthy remote platform that can verify the provided integrity and confidentiality of the send data, so that the exchanged data becomes accessible.

The encryption ensures confidentiality and integrity of transferred data by the usage of robust crypto-algorithms given by OT.Crypt. On the other side OE.RP_Trans ensures that the remote platform provides adequate mechanisms to ensure the confidentiality and integrity of data transferred between the TOE and itself.

T.Mobile_Agent (Modification or eavesdropping of mobile agent data during transfer) is encountered by OT.RP_Data_Receive which ensures that a mobile agent is only accepted from a trustworthy remote platform after a successful verification of integrity and confidentiality. On the other side OT.RP_Data_Send ensures that a mobile agent will only be send to the intended trustworthy remote platform that can verify the provided integrity and confidentiality of the send data, so that the exchanged data becomes accessible.

The encryption ensures confidentiality and integrity of transferred data by the usage of robust crypto-algorithms given by OT.Crypt. On the other side OE.RP_Trans ensures that the remote platform provides adequate mechanisms to ensure the confidentiality and integrity of data transferred between the TOE and itself.

T.User_Data (Modification or eavesdropping of user data during transfer) is encountered by OT.UI_Data_Receive and OT.UI_Data_Send by which the TOE has the possibility to verify integrity and confidentiality of the data received from a trustworthy user interface. Also the TOE does only send user application data when the ability is given that integrity and confidentiality can be verified by the intended trustworthy remote user interface.

The encryption ensures confidentiality and integrity of transferred data by the usage of robust crypto-algorithms given by OT.Crypt.

T.CA_Data (Modification of certificate and certificate revocation list (CRL) during transfer) is encountered by OT.Trusted_CA by which the TOE can detect spoofing of a trustworthy Certification Authority by an illicit third party and if modification of the transmitted certificates or certificate revocation list took place.

OE.CA_Cert claims that the Certification Authority generates and provides valid certificates over trustworthy remote platforms and user interfaces as well as provides the certificate revocation list.

The integrity of the data is ensured by a signed data (certificates and CRL) generated by the CA (OE.CA_Cert) which are verified by the TOE (OT.Trusted_CA). Additionally an encryption during the data transfer between the CA and the TOE takes place ensuring confidentiality and integrity of transferred data by the usage of robust crypto-algorithms given by OT.Crypt.

8.1.2.3. Assumptions and Security Objective Sufficiency

A.CA_Cert (CA generates platform certificates and a certificate revocation list (CRL)) is counter measured by OE.CA_Cert which claims that the Certification Authority generates and provides certificates over trustworthy remote platforms and user interfaces as well as the certificate revocation list. The CA ensures the trustworthiness of the RP and UI by taking appropriate organisational measures.

A.User_Interface (Trustworthy user interface for application creation) is counter measured by OE.UI_Trust which claims that the user interface maintains integrity and confidentiality of user identification and authentication data as well as user application data by adequate measures. Further more it is demanded by OE.UI_Trans that the user interface only sends this identification and authentication data and application data to the TOE.

A.Remote_Platform (Trustworthy remote platform) is counter measured by OE.RP_Trust which claims that a trustworthy remote platform solely sends speech act and mobile agent data and that these data do not contain any malicious or illicit data.

A.Access (Limited physical and logical access) is counter measured by OE.Restricted_Acces which limits the physical access to the TOE to authorised persons (the Administrator) only and ensures that the direct physical access is the only way to administer the TOE and that the IT-Environment (HW, OS) has to ensure the protection of the resource used by the TOE against external attacks.

8.2. Security requirements rationale

8.2.1. Security Requirement Coverage

TOE Security Functional Requirements / TOE Security Objectives	OT.Crypt	OT.Data_Receive	OT.Data_Send	OT.RP_Data_Receive	OT.RP_Data_Send	OT.UI_Data_Receive	OT.UI_Data_Send	OT.Trusted_CA
FCO_NRO.1								x
FCS_CKM.1	x							
FCS_CKM.4	x							
FCS_COP.1 / SSL	x			x	x	x	x	x
FCS_COP.1 / sig_verify	x							x
FDP_ACC.1 / UI						x	x	
FDP_ACF.1 / UI						x	x	
FDP_ACC.1 / RP				x	x			
FDP_ACF.1 / RP				x	x			
FDP_ACC.1 / LDAP		x	x					
FDP_ACF.1 / LDAP		x	x					
FDP_ACC.1 / CA								x
FDP_ACF.1 / CA								x

TOE Security Functional Requirements / TOE Security Objectives	OT.Crypt	OT.Data_Receive	OT.Data_Send	OT.RP_Data_Receive	OT.RP_Data_Send	OT.UI_Data_Receive	OT.UI_Data_Send	OT.Trusted_CA
FDP_ETC.1			x		x			x
FDP_ETC.2 / RP					x			
FDP_ETC.2 / UI							x	
FDP_ITC.1		x		x				
FDP_ITC.2 / RP				x				
FDP_ITC.2 / CA								x
FDP_ITC.2 / UI						x		
FDP_SDI.2	x							x
FDP_UIT.1				x	x	x	x	x
FIA_ATD.1						x	x	
FIA_SOS.1						x	x	
FIA_UAU.1 / human						x	x	
FIA_UAU.1 / entity				x	x	x	x	x
FIA_UID.1 / human						x	x	
FIA_UID.1 / entity				x	x	x	x	x
FIA_USB.1						x	x	
FMT_MOF.1 / external		x	x	x	x	x	x	x
FMT_MOF.1 / admin						x	x	
FMT_MOF.1 / user						x	x	
FMT_MSA.1		x	x	x	x	x	x	x
FMT_MSA.2				x	x	x	x	x
FMT_MSA.3		x	x	x	x	x	x	x
FMT_MTD.1 / Auth						x	x	
FMT_MTD.1 / I&A						x	x	
FMT_MTD.1 / key-pair	x							
FMT_MTD.1 / CA-key								x
FMT_SMF.1				x	x	x	x	x
FMT_SMR.1						x	x	
FPT_FLS.1		x	x	x	x	x	x	x
FPT_TDC.1 / signature								x
FPT_TDC.1 / I&A						x	x	
FPT_TDC.1 / service-ID						x	x	
FTP_ITC.1				x	x	x	x	x
FTP_TRP.1						x	x	

Table 7: Functional Requirement to TOE Security Objective Mapping

Environment Security Requirement / Environment Security Objectives	OE.Restricted_Access	OE.CA_Cert	OE.RP_Trust	OE.RP_Trans	OE.UI_Trust	OE.UI_Trans
FCS_COP.1 / E-SSL		x		x		x
FCS_COP.1 / E-sign		x				
FCO_NRO.1 / E-CA		x				
FTP_ITC.1 / E		x		x		x
R.Restricted_Access	x					
R.CA_Key_Management	x	x				
R.CA_Certificate		x				
R.RP_Management			x			
R.UI_Management					x	
R.Service_Agents	x					

Table 8: IT Environment Functional requirements to Environment Security Objective Mapping

8.2.2. Security Requirements Sufficiency

8.2.2.1. TOE Security Requirements Sufficiency

OT.Crypt (Usage of robust encryption and signing techniques) is addressed by FCS_CKM.1 which generates the RSA key-pair of the TOE (local platform) with a key length of 1024 or 2048 bit. Signatures are verified by FCS_COP.1 / sig_verify using RSA with key length of 1024 or 2048 bit and the hash algorithm SHA-1.

Keys that are no longer used are deleted by zeroisation provided by FCS_CKM.4.

The underlying SSL protocol specified by FCS_COP.1 / SSL provides the necessary robustness for the data encryption during transfer.

The private keys stored within the TOE are integrity protected by FDP_SDI.2. The management (creation and deletion) of the RSA keys is restricted to the Administrator only as specified in FMT_MTD.1 / key-pair.

OT.Data_Receive (Reliability of received data) is addressed by FDP_ACF.1 / LDAP and FDP_ACC.1 / LDAP ensuring that data with unknown or unreliable origin are only accepted as LDAP data. These imply all transmitted plain text data. In case of a platform failure a breach in this rule will be prevented by FPT_FLS.1. The Administrator is also allowed to enable and disable external communication FMT_MOF.1 / external.

The imported data do not contain any associated security attributes as required by FDP_ITC.1.

FMT_MSA.3 requires that the TOE assures that the security attribute are initialised with restrictive default values (“trusted SSL connect” set to “no” and “role” set to “none”). FMT_MSA.1 requires that these attributes cannot be modified by any authorised user as Administrator or any human user, but are set in dependency of the successful establishment

of a SSL connection based on a successful verification of the entities (“role”) certificate provided by the CA.

OT.Data_Send (Confidentiality of send data) is addressed by FDP_ACF.1 / LDAP and FDP_ACC.1 / LDAP ensuring that data send over a not secured communication channel are only information for an LDAP. These imply all transmitted plain text data. In case of a platform failure a breach in this rule will be prevented by FPT_FLS.1. The Administrator is also allowed to enable and disable external communication FMT_MOF.1 / external.

The exported data do not contain any associated security attributes as required by FDP_ETC.1.

FMT_MSA.3 requires that the TOE assures that the security attribute are initialised with restrictive default values (“trusted SSL connect” set to “no” and “role” set to “none”). FMT_MSA.1 requires that these attributes cannot be modified by any authorised user as Administrator or any human user, but are set in dependency of the successful establishment of a SSL connection based on a successful verification of the entities (“role”) certificate provided by the CA.

OT.RP_Data_Receive (Mobile agent or speech act data received by a remote platform) is addressed by FDP_ACC.1 / RP and FDP_ACF.1 / RP ensuring that the TOE only accepts SSL protected data send by a trustworthy remote platform (RP) as mobile agent or speech act data. Mobile agent data received by a remote platform must include an associated service-ID as required by FDP_ITC.2 / RP whereas speech act data are imported without security attributes specified in FDP_ITC.1.

The underlying SSL protocol specified by FCS_COP.1 / SSL establishes a trusted channel FTP_ITC.1 which ensures the confidentiality and integrity during the data transfer and also ensures the protection from modification, deletion, insertion, and replay errors as required by FDP_UIT.1.

Further security management functionalities that are performed by the TOE can be found in the specification of FMT_SMF.1.

The remote platform has to be identified and authenticated as required in FIA_UAU.1 / entity and FIA_UID.1 / entity.

FMT_MSA.3 requires that the TOE assures that the security attribute are initialised with restrictive default values (“trusted SSL connect” set to “no” and “role” set to “none”). FMT_MSA.1 requires that these attributes cannot be modified by any authorised user as Administrator or any human user, but are set in dependency of the successful establishment of a SSL connection based on a successful verification of the entities (“role”) certificate provided by the CA.

FMT_MSA.2 requires that for the key length of the security attribute only sufficient values are accepted.

In case of a platform failure FPT_FLS.1 stops external communication to provide a security leakage. The Administrator is also allowed to enable and disable external communication FMT_MOF.1 / external.

OT.RP_Data_Send (Mobile agent or speech act data send to a remote platform) is addressed by FDP_ACC.1 / RP and FDP_ACF.1 / RP ensuring that the TOE only sends mobile agent or speech act data protected by SSL to a trustworthy remote platform (RP). Mobile agent data send by a remote platform must include an associated service-ID as required by FDP_ETC.2 / RP whereas speech act data are exported without security attributes specified in FDP_ETC.1.

The underlying SSL protocol specified by FCS_COP.1 / SSL establishes a trusted channel FTP_ITC.1 which ensures the confidentiality and integrity during the data transfer and also ensures the protection from modification, deletion, insertion, and replay errors as required by FDP_UIT.1.

Further security management functionalities that are performed by the TOE can be found in the specification of FMT_SMF.1.

The remote platform has to be identified and authenticated as required in FIA_UAU.1 / entity and FIA_UID.1 / entity.

FMT_MSA.3 requires that the TOE assures that the security attribute are initialised with restrictive default values ("trusted SSL connect" set to "no" and "role" set to "none"). FMT_MSA.1 requires that these attributes cannot be modified by any authorised user as Administrator or any human user, but are set in dependency of the successful establishment of a SSL connection based on a successful verification of the entities ("role") certificate provided by the CA.

FMT_MSA.2 requires that for the key length of the security attribute only sufficient values are accepted.

In case of a platform failure FPT_FLS.1 stops external communication to provide a security leakage. The Administrator is also allowed to enable and disable external communication FMT_MOF.1 / external.

OT.UI_Data_Receive (User application data received by a user interface) is addressed by FDP_ACC.1 / UI and FDP_ACF.1 / UI ensuring that the TOE only accepts SSL protected data send by a trustworthy remote user interface (UI) as user application data or identification and authentication data.

The underlying SSL protocol specified by FCS_COP.1 / SSL establishes a trusted channel FTP_ITC.1 which ensures the confidentiality and integrity during the transfer and also ensures the protection from modification, deletion, insertion, and replay errors as required by FDP_UIT.1.

The trusted channel is established before the identification and authentication process is carried out by FIA_UAU.1 / human and FIA_UID.1 / human and is used as a trusted path as specified in FTP_TRP.1 to import the identity of the human user within the identification and authentication data FDP_ITC.2 / UI.

The Administrator has the ability to create and delete user identification and authentication data and therefore user roles as stated in FMT_MTD.1 / I&A. The human user being associated to this role has the ability to change his authentication data as stated in FMT_MTD.1 / Auth. FPT_TDC.1 / I&A and FIA_SOS.1 provides the verification of user identification and authentication data with aid of the internally stored reference data.

The Administrator is allowed to generate, delete, modify or monitor (service) agents as required by FMT_MOF.1 / admin. Such an agent allows a user to initiate a service acting on his behalf FMT_MOF.1 / user. This service is attached with a unique service-ID associated

with this user FIA_USB.1. The TOE provides the maintenance of the user roles as specified in FMT_SMR.1. Furthermore the service-ID / user binding is maintained by the TOE as required by FIA_ATD.1 and FPT_TDC.1 / service-ID.

Further security management functionalities that are performed by the TOE can be found in the specification of FMT_SMF.1.

The user interface has to be identified and authenticated as required in FIA_UAU.1 / entity and FIA_UID.1 / entity.

FMT_MSA.3 requires that the TOE assures that the security attribute are initialised with restrictive default values ("trusted SSL connect" set to "no" and "role" set to "none"). FMT_MSA.1 requires that these attributes cannot be modified by any authorised user as Administrator or any human user, but are set in dependency of the successful establishment of a SSL connection based on a successful verification of the entities ("role") certificate provided by the CA.

FMT_MSA.2 requires that for the key length of the security attribute only sufficient values are accepted.

In case of a platform failure FPT_FLS.1 stops external communication to provide a leakage of security. The Administrator is also allowed to enable and disable external communication FMT_MOF.1 / external.

OT.UI_Data_Send (User application data send to a user interface) is addressed by FDP_ACC.1 / UI and FDP_ACF.1 / UI ensuring that the TOE only sends SSL protected user application data or identification data to a trustworthy remote user interface (UI).

The underlying SSL protocol specified by FCS_COP.1 / SSL establishes a trusted channel FTP_ITC.1 which ensures the confidentiality and integrity during the transfer and also ensures the protection from modification, deletion, insertion, and replay errors as required by FDP_UIT.1.

The trusted channel is established before the identification and authentication process is carried out by FIA_UAU.1 / human and FIA_UID.1 / human and is used as a trusted path as specified in FTP_TRP.1 to export the identity of the human user within the user application data FDP_ETC.2 / UI.

The Administrator has the ability to create and delete user identification and authentication data and therefore user roles as stated in FMT_MTD.1 / I&A. The human user being associated to this role has the ability to change his authentication data as stated in FMT_MTD.1 / Auth. FPT_TDC.1 / I&A and FIA_SOS.1 provides the verification of user identification and authentication data with aid of the internally stored reference data.

The Administrator is allowed to generate, delete, modify or monitor (service) agents as required by FMT_MOF.1 / admin. A user can query the status of any service acting on his behalf executed by a service agent FMT_MOF.1 / user. This service is attached with a unique service-ID associated with this user FIA_USB.1. The TOE provides the maintenance of the user roles as specified in FMT_SMR.1. Furthermore the service-ID / user binding is maintained by the TOE as required by FIA_ATD.1 and FPT_TDC.1 / service-ID.

Further security management functionalities that are performed by the TOE can be found in the specification of FMT_SMF.1.

The user interface has to be identified and authenticated as required in FIA_UAU.1 / entity and FIA_UID.1 / entity.

FMT_MSA.3 requires that the TOE assures that the security attribute are initialised with restrictive default values (“trusted SSL connect” set to “no” and “role” set to “none”). FMT_MSA.1 requires that these attributes cannot be modified by any authorised user as Administrator or any human user, but are set in dependency of the successful establishment of a SSL connection based on a successful verification of the entities (“role”) certificate provided by the CA.

FMT_MSA.2 requires that for the key length of the security attribute only sufficient values are accepted.

In case of a platform failure FPT_FLS.1 stops external communication to provide a leakage of security. The Administrator is also allowed to enable and disable external communication FMT_MOF.1 / external.

OT.Trusted_CA (Spoofing of a trustworthy Certification Authority) is addressed by FCO_NRO.1 ensuring that certificates and the certificate revocation list (CRL) are generated and signed by the Certification Authority (CA) as originator.

The signatures are imported within the certificates and CRLs as required by FDP_ITC.2 / CA and verified as specified in FPT_TDC.1 /signature using the cryptographic operations specified in FCS_COP.1 / sig_verify.

The SSL protected data transmission to the CA allows the import of certificates and CRLs from a trustworthy CA and restricts the import of CRLs to trustworthy CAs only as required by FDP_ACC.1 / CA and FDP_ACF.1 / CA.

The underlying SSL protocol specified by FCS_COP.1 / SSL establishes a trusted channel FTP_ITC.1 which ensures the confidentiality and integrity during the transfer and also ensures the protection from modification, deletion, insertion, and replay errors as required by FDP_UIT.1. Data being exported to the CA are send without any security attributes as in FDP_ETC.1.

The CA’s public key used for the verification of the signatures is stored within the TOE is integrity protected by FDP_SDI.2 and can only be imported or modified by the Administrator as required by FMT_MTD.1 / CA-key.

Further security management functionalities that are performed by the TOE can be found in the specification of FMT_SMF.1.

The Certification Authority has to be identified and authenticated as required in FIA_UAU.1 / entity and FIA_UID.1 / entity.

FMT_MSA.3 requires that the TOE assures that the security attribute are initialised with restrictive default values (“trusted SSL connect” set to “no” and “role” set to “none”). FMT_MSA.1 requires that these attributes cannot be modified by any authorised user as Administrator or any human user, but are set in dependency of the successful establishment of a SSL connection based on a successful verification of the entities (“role”) certificate provided by the CA.

FMT_MSA.2 requires that for the key length of the security attribute only sufficient values are accepted.

In case of a platform failure FPT_FLS.1 stops external communication to provide a security leakage. The Administrator is also allowed to enable and disable external communication FMT_MOF.1 / external.

8.2.2.2. TOE Environment Security Requirements Sufficiency

OE.Restricted_Access (Physical and logical access to the TOE) as required by R.Restricted_Access physical access to the TOE is only allowed for the Administrator of that platform. The direct physical access is the only way to administer the TOE. Also the IT-Environment (HW, OS) has to ensure the protection of the resources used by the TOE against external attacks.

Further more the Administrator has to provide adequate organisational methods for key distribution and import. Adequate organisational methods for key distribution are specified in R.CA_Key_Management and cover especially the integrity protected export of the local platform's public key and the import of the Certification Authority's public key. This is important to support logical access also required by R.Restricted_Access used to modify the security attributes when establishing a connection outside the TOE after verifying data (trustworthy certificates and CRL) provided by the CA in accordance with the internally stored public key of the CA.

By implementing new service agents on the TOE, the Administrator has to ensure that these are TOE conform service agents, which are not containing or bypassing any TOE security functionality as required by R.Service_Agents.

OE.CA_Cert (Certificates and CRL as generated by the Certification Authority) requires that reliable and unforgeable certificates over trustworthy remote platforms and trustworthy user interfaces are generated by a Certification Authority as identified in R.CA_Certificate. These data must be signed in accordance with FCS_COP.1 / E-sign to ensure data integrity the possibility to verify the origin of the provided data.

This data are only transferred between the TOE and the Certification Authority via a secure communication channel that meets the specifications in FCS_COP.1 / E-SSL. The communication channel established between the Certification Authority and the TOE needs to meet the requirements as specified in FTP_ITC.1 / E which assures identification of both end points and protection from modification or disclosure. Evidence of origin for transmitted data between the Certification Authority and the TOE is assured by FCO_NRO.1 / E-CA.

Adequate organisational methods for key distribution are specified in R.CA_Key_Management and cover especially the integrity protected export of the local platform's public key and the import of the Certification Authority's public key.

OE.RP_Trust (Trusted remote platform environment) requires that a trustworthy remote platform solely sends speech act and mobile agent data and that these data do not contain any malicious or illicit data as defined in R.RP_Management.

OE.RP_Trans (Secure data transfer to and from the remote platform) requires that only data are transferred between the TOE and the trustworthy remote platform via a secure communication channel that meets the specifications in FCS_COP.1 / E-SSL. The communication channel established between the trustworthy remote platform and the TOE needs to meet the requirements as specified in FTP_ITC.1 / E which assures identification of both end points and protection from modification or disclosure.

OE.UI_Trust (Trusted remote user interface environment) requires that the trustworthy user interface maintains the integrity and confidentiality of data for the identification and authentication of the human user and of the user application as defined in R.UI_Management.

OE.UI_Trans (Secure data transfer to and from the remote user interface) requires that only data are transferred between the TOE and the trustworthy user interface via a secure communication channel that meets the specifications in FCS_COP.1 / E-SSL. The communication channel established between the trustworthy user interface and the TOE needs to meet the requirements as specified in FTP_ITC.1 / E which assures identification of both end points and protection from modification or disclosure.

8.3. Dependency Rationale

8.3.1. Functional and Assurance Requirements Dependencies

The assurance requirements' dependencies for the TOE are completely fulfilled. The functional requirements' dependencies for the TOE environment are not completely fulfilled (see the next section for justification).

Requirement	Dependencies	Supported dependencies
Functional Requirements for the TOE		
FCO_NRO.1	FIA_UID.1	FIA_UID.1 / entity
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 FMT_MSA.2	FCS_COP.1 / SSL FCS_CKM.4 FMT_MSA.2
FCS_CKM.4	[FDP_ITC.1 or FCS_CKM.1] FMT_MSA.2	FCS_CKM.1 FMT_MSA.2
FCS_COP.1 / SSL	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2
FCS_COP.1 / sig_verify	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	FCS_CKM.1 FCS_CKM.4 FMT_MSA.2
FDP_ACC.1 / UI	FDP_ACF.1	FDP_ACF.1 / UI
FDP_ACF.1 / UI	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 / UI FMT_MSA.3
FDP_ACC.1 / RP	FDP_ACF.1	FDP_ACF.1 / RP
FDP_ACF.1 / RP	FDP_ACC.1	FDP_ACC.1 / RP

Requirement	Dependencies	Supported dependencies
	FMT_MSA.3	FMT_MSA.3
FDP_ACC.1 / LDAP	FDP_ACF.1	FDP_ACF.1 / LDAP
FDP_ACF.1 / LDAP	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 / LDAP FMT_MSA.3
FDP_ACC.1 / CA	FDP_ACF.1	FDP_ACF.1 / CA
FDP_ACF.1 / CA	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 / CA FMT_MSA.3
FDP_ETC.1	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1 / RP, / CA, / LDAP
FDP_ETC.2 / RP	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1 / RP
FDP_ETC.2 / UI	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1 / UI
FDP_ITC.1	[FDP_ACC.1 or FDP_IFC.1] FMT_MSA.3	FDP_ACC.1 / RP, / LDAP FMT_MSA.3
FDP_ITC.2 / RP	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	FDP_ACC.1 / RP FTP_ITC.1 FPT_TDC.1 / service-ID
FDP_ITC.2 / CA	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	FDP_ACC.1 / CA FTP_ITC.1 FPT_TDC.1 / signature
FDP_ITC.2 / UI	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1] FPT_TDC.1	FDP_ACC.1 / UI FTP_ITC.1 and FTP_TRP.1 FPT_TDC.1 / I&A
FDP_SDI.2	_	_
FDP_UIT.1	[FDP_ACC.1 or FDP_IFC.1] [FTP_ITC.1 or FTP_TRP.1]	FDP_ACC.1 / RP, / UI, / CA FTP_ITC.1 and FTP_TRP.1
FIA_ATD.1	_	_
FIA_SOS.1	_	_
FIA_UAU.1 / human	FIA_UID.1	FIA_UID.1 / human
FIA_UAU.1 / entity	FIA_UID.1	FIA_UID.1 / entity
FIA_UID.1 / human	_	_
FIA_UID.1 / entity	_	_
FIA_USB.1	FIA_ATD.1	FIA_ATD.1

Requirement	Dependencies	Supported dependencies
FMT_MOF.1 / external	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MOF.1 / admin	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MOF.1 / user	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMF.1 FMT_SMR.1	FDP_ACC.1 / RP, / UI, / CA, / LDAP FMT_SMF.1 FMT_SMR.1
FMT_MSA.2	ADV_SPM.1 [FDP_ACC.1 or FDP_IFC.1] FMT_MSA.1 FMT_SMR.1	(see 8.3.2 for a rationale) FDP_ACC.1 / RP, / UI, / CA, / LDAP FMT_MSA.1 FMT_SMR.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1 / Auth	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1 / I&A	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1 / key-pair	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1 / CA-key	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	_	_
FMT_SMR.1	FIA_UID.1	FIA_UID.1 / human, / entity
FPT_FLS.1	ADV_SPM.1	(see 8.3.2 for a rationale)
FPT_TDC.1 / signature	_	_
FPT_TDC.1 / I&A	_	_
FPT_TDC.1 / service-ID	_	_
FTP_ITC.1	_	_

Requirement	Dependencies	Supported dependencies
FTP_TRP.1	–	–
Assurance Requirements		
ACM_CAP.3	(FI 095: ACM_SCP.1), ALC_DVS.1	(FI 095: ACM_SCP.1), ALC_DVS.1
ACM_SCP.1	ACM_CAP.3	ACM_CAP.3
ADO_DEL.1	no dep.	no dep.
ADO_IGS.1	no dep	no dep
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1
ADV_HLD.2	ADV_FSP.1, ADV_RCR.1	ADV_FSP.1, ADV_RCR.1
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1	ADV_FSP.1
ALC_DVS.1	no dep.	no dep.
ATE_COV.2	ADV_FSP.1, ATE_FUN.1	ADV_FSP.1, ATE_FUN.1
ATE_DPT.1	ADV_HLD.1, ATE_FUN.1	ADV_HLD.1, ATE_FUN.1
ATE_FUN.1	no dep.	no dep.
ATE_IND.2	ADV_FSP.1, AGD_USR.1, ATE_FUN.1	ADV_FSP.1, AGD_USR.1, ATE_FUN.1
AVA_MSU.1	ADO_IGS.1, ADV_FSP.1, AGD_USR.1	ADO_IGS.1, ADV_FSP.1, AGD_USR.1
AVA_SOF.1	ADV_FSP.1, ADV_HLD.1	ADV_FSP.1, ADV_HLD.1
AVA_VLA.1	ADV_FSP.1, ADV_HLD.1, AGD_USR.1	ADV_FSP.1, ADV_HLD.1, AGD_USR.1
Functional Requirements for the IT-Environment		
FCS_COP.1 / E-SSL	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	–
FCS_COP.1 / E-sign	[FDP_ITC.1 or FCS_CKM.1] FCS_CKM.4 FMT_MSA.2	–
FCO_NRO.1 / E-CA	FIA_UID.1	–
FTP_ITC.1 / E	–	–

Table 9: Functional and Assurance Requirements Dependencies

8.3.2. Justification of Unsupported Dependencies

The following dependencies are not fulfilled by the TSFRs given in 5.1:

- The requirement ADV_SPM.1 (informal security policy model) ask for by FPT_MSA.2 and FPT_FLS.1 will not explicitly be stated for this TOE. The reason is that the TOE's security policy is rather simple. The TSP only comprises the establishment of a SSL protected communication channel basing on the identification of trustworthy entities. The two attributes "role" and trusted SSL connect" are set by simple decisions. Its details are already stated in the TOE description in section 2, especially there in section 2.2 and in the definition of the TSF 6.1. The secure state required by FPT_FLS.1 is realised by stopping all external communications in case an error occurs on which the platform cannot react in an appropriate manner. Only the Administrator is able to start the external communication again. It is not needed to describe this behaviour within a security policy model.

The following dependencies are not fulfilled by the ESFRs given in 5.3:

- The requirement [FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4 and FMT_MSA.2 ask for by FCS_COP.1 / E-SSL and FCS_COP.1 / E-sign will not explicitly be stated for this TOE, because the key-generation, -deletion and the management of security attributes from trustworthy remote platform, trustworthy remote user interfaces and the Certification Authority is out of scope of the TOE.
- The requirement FIA_UID.1 ask for by FCO_NRO.1 / E-CA will not explicitly be stated for this TOE, because the non repudiation of origin refers to the Certification Authority as an instance respectively as an entity and not as a human user. Furthermore, the timing of user identification is out of the scope of the TOE and not necessary here.

8.4. Security Requirements Grounding in Objectives

This chapter covers the grounding that has not been done in the precedent chapter.

Requirement	Security Objectives
Security Assurance Requirements	
ACM_CAP.3	EAL 3
ACM_SCP.1	EAL 3
ADO_DEL.1	EAL 3
ADO_IGS.1	EAL 3
ADV_FSP.1	EAL 3
ADV_HLD.2	EAL 3
ADV_RCR.1	EAL 3
AGD_ADM.1	EAL 3
AGD_USR.1	EAL 3
ALC_DVS.1	EAL 3
ATE_COV.2	EAL 3

Requirement	Security Objectives
ATE_DPT.1	EAL 3
ATE_FUN.1	EAL 3
ATE_IND.2	EAL 3
AVA_MSU.1	EAL 3
AVA_SOF.1	EAL 3
AVA_VLA.1	EAL 3

Table 10: Assurance Requirement to Security Objective Mapping

8.5. TOE summary specification rationale

8.5.1. Security Function Coverage

TOE Security Functional Requirements/TOE Security Functions	SF 1 User communication	SF 2 Remote platform Speech-act transmission	SF 3 LDAP based data exchange	SF 4 Mobile agent transmission	SF 5 Certificate and key management
FCO_NRO.1					x
FCS_CKM.1					x
FCS_CKM.4					x
FCS_COP.1 / SSL	x	x		x	x
FCS_COP.1 / sig_verify					x
FDP_ACC.1 / UI	x				
FDP_ACF.1 / UI	x				
FDP_ACC.1 / RP		x		x	
FDP_ACF.1 / RP		x		x	
FDP_ACC.1 / LDAP			x		
FDP_ACF.1 / LDAP			x		
FDP_ACC.1 / CA					x
FDP_ACF.1 / CA					x
FDP_ETC.1		x	x		x
FDP_ETC.2 / RP				x	
FDP_ETC.2 / UI	x				
FDP_ITC.1		x	x		
FDP_ITC.2 / RP				x	
FDP_ITC.2 / CA					x
FDP_ITC.2 / UI	x				
FDP_SDI.2					x

TOE Security Functional Requirements/TOE Security Functions	SF 1 User communication	SF 2 Remote platform Speech-act transmission	SF 3 LDAP based data exchange	SF 4 Mobile agent transmission	SF 5 Certificate and key management
FDP_UIT.1	x	x		x	x
FIA_ATD.1	x			x	
FIA_SOS.1	x				
FIA_UAU.1 / human	x				
FIA_UAU.1 / entity	x	x		x	x
FIA_UID.1 / human	x				
FIA_UID.1 / entity	x	x		x	x
FIA_USB.1	x				
FMT_MOF 1 / external	x	x	x	x	x
FMT_MOF.1 / admin	x	x	x	x	x
FMT_MOF.1 / user	x				
FMT_MSA.1	x	x	x	x	x
FMT_MSA.2	x	x		x	x
FMT_MSA.3	x	x	x	x	x
FMT_MTD.1 / Auth	x				
FMT_MTD.1 / I&A	x				
FMT_MTD.1 / key-pair					x
FMT_MTD.1 / CA-key					x
FMT_SMF.1	x	x	x	x	x
FMT_SMR.1	x				
FPT_FLS.1	x	x	x	x	x
FPT_TDC.1 / signature					x
FPT_TDC.1 / I&A	x				
FPT_TDC.1 / service-ID	x			x	
FTP_ITC.1	x	x		x	x
FTP_TRP.1	x				

Table 11: TOE security function to TOE security functional requirement mapping

8.5.2. TOE Security Function Sufficiency

Each TOE security functional requirement is implemented by at least one security function. How and whether the security functions actually implement the TOE security functional requirement is described in sec. 6.1.

TOE Security Functional Requirements/TOE Security Functions	SSL connection (SF1, 2, 4, 5)	Entity I&A (SF1, 2, 4, 5)	Error and Platform Manage–ment (SF1, 2, 3, 4, 5)	Access Control (SF1)	Human I&A (SF1)	Access Control (SF2)	Access Control (SF3)	Management of Security Attributes (SF3)	Access Control (SF4)	Access Control (SF5)	Key Management (SF5)	Verification of Signature (SF5)
FCO_NRO.1												x
FCS_CKM.1											x	
FCS_CKM.4											x	
FCS_COP.1 / SSL	x											
FCS_COP.1 / sig_verify												x
FDP_ACC.1 / UI				x								
FDP_ACF.1 / UI				x								
FDP_ACC.1 / RP						x			x			
FDP_ACF.1 / RP						x			x			
FDP_ACC.1 / LDAP							x					
FDP_ACF.1 / LDAP							x					
FDP_ACC.1 / CA										x		
FDP_ACF.1 / CA										x		
FDP_ETC.1						x	x			x		
FDP_ETC.2 / RP									x			
FDP_ETC.2 / UI				x								
FDP_ITC.1						x	x					
FDP_ITC.2 / RP									x			
FDP_ITC.2 / CA										x		
FDP_ITC.2 / UI				x								
FDP_SDI.2											x	
FDP_UIT.1	x											
FIA_ATD.1					x				x			
FIA_SOS.1					x							
FIA_UAU.1 / human					x							
FIA_UAU.1 / entity		x										
FIA_UID.1 / human					x							
FIA_UID.1 / entity		x										
FIA_USB.1					x							
FMT_MOF 1 / external			x									
FMT_MOF.1 / admin			x									
FMT_MOF.1 / user					x							
FMT_MSA.1		x						x				
FMT_MSA.2	x											
FMT_MSA.3		x						x				
FMT_MTD.1 / Auth					x							
FMT_MTD.1 / I&A					x							

TOE Security Functional Requirements/TOE Security Functions	SSL connection (SF1, 2, 4, 5)	Entity I&A (SF1, 2, 4, 5)	Error and Platform Manage–ment (SF1, 2, 3, 4, 5)	Access Control (SF1)	Human I&A (SF1)	Access Control (SF2)	Access Control (SF3)	Management of Security Attributes (SF3)	Access Control (SF4)	Access Control (SF5)	Key Management (SF5)	Verification of Signature (SF5)
FMT_MTD.1 / key-pair											x	
FMT_MTD.1 / CA-key											x	
FMT_SMF.1			x		x						x	
FMT_SMR.1					x							
FPT_FLS.1			x									
FPT_TDC.1 / signature												x
FPT_TDC.1 / I&A					x							
FPT_TDC.1 / service-ID					x				x			
FTP_ITC.1	x											
FTP_TRP.1				x								

Table 12: TOE security function to TOE security functional requirement mapping

8.5.3. Assurance measures rationale

TOE Security Assurance Requirements	TOE Assurance Measures
ACM_CAP.3	ACM_CAP.3M
ACM_SCP.1	ACM_SCP.1M
ADO_DEL.1	ADO_DEL.1M
ADO_IGS.1	ADO_IGS.1M
ADV_FSP.1	ADV_FSP.2M
ADV_HLD.2	ADV_HLD.2M
ADV_RCR.1	ADV_RCR.1M
AGD_ADM.1	AGD_ADM.1M
AGD_USR.1	AGD_USR.1M
ALC_DVS.1	ALC_DVS.1M
ATE_COV.2	ATE_COV.2M
ATE_DPT.1	ATE_DPT.1M
ATE_FUN.1	ATE_FUN.1M
ATE_IND.2	ATE_IND.2M
AVA_MSU.1	AVA_MSU.1M

TOE Security Assurance Requirements	TOE Assurance Measures
AVA_SOF.1	AVA_SOF.1M
AVA_VLA.1	AVA_VLA.1M

Table 13: Mapping TOE Security Assurance Requirements to TOE Assurance Measures

Each TOE security assurance requirement is implemented by exactly one assurance measure. The content and application of these assurance measures exactly accords with the assurance components of CC part 3 [3] with the same identifier, respectively, and CEM [4].

8.5.4. Mutual supportiveness of the Security Functions

The TOE security functions are mutual supportive.

User communication (SF1) needs certificate and key management (SF5) for verification of the trustworthiness of remote user interfaces because of the certificates and the certificate revocation list that the Certification Authority provides. Further more User communication (SF1) uses LDAP based data exchange (SF3) to register data and to access address-information about registered agents on known platforms.

Remote platform speech act transmission (SF2) needs certificate and key management (SF5) for verification of the trustworthiness of remote user interfaces because of the certificates and the certificate revocation list that the Certification Authority provides. Further more the remote platform (SF1) uses LDAP based data exchange (SF3) to register data and to access address-information about registered agents on known platforms.

Mobile agent transmission (SF4) needs certificate and key management (SF5) for verification of the trustworthiness of remote platforms because of the certificates and the certificate revocation list that the Certification Authority provides. Further more the remote platform (SF1) uses LDAP based data exchange (SF3) to register data and to access address-information about registered agents on known platforms.

This context is represented in the following table:

SF	Function	SF	Uses function(s)
SF1	User communication	SF5 SF3	Certificate and key management LDAP based data exchange
SF2	Remote platform speech act transmission	SF5 SF3	Certificate and key management LDAP based data exchange
SF3	LDAP based data exchange		
SF4	Mobile agent transmission	SF5 SF3	Certificate and key management LDAP based data exchange
SF5	Certificate and key management		

Table 14: Mutual supportiveness of the security functions.

8.6. Rationale for Extensions

The ST does not use extensions to the CC part 2 [2].

8.7. Rationale for Evaluation Assurance Level 3

The level EAL3 is chosen in order to meet assurance expectations for commercial products that can be applied to telecommunication and telematic backgrounds.

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.

The threats defined in the security target address obvious attack methods and threat agents which do not need any specialised knowledge to perform the respective attack. Therefore this fits to the analysis of the construction and the vulnerability analysis to be resistant against obvious vulnerabilities.

No augmentation has been chosen.

8.8. Rationale for Strength of Function Basic

The TOE shall demonstrate to be resistant against attacks addressing obvious vulnerabilities. The protection against those attacks dictates no strength of function rating. Nevertheless for functions in the TOE that are realised by probabilistic or permutational mechanisms SOF-basic is claimed.

There are two identified probabilistic or permutational mechanisms:

- The password mechanism for the User identification and authentication (permutational).
- A pseudo (deterministic) random number generator (PRNG) used for key generation and challenge generation during the SSL handshake (probabilistic). This mechanism will be assessed according the AIS20.

All other probabilistic or permutational mechanisms in order to meet the security objective OT.Crypt are cryptographic mechanisms and must not be assessed within this Strength of Function analysis.

8.9. PP claims rationale

The PP claims rationale statement shall explain any difference between the ST security objectives and requirements and those of any PP to which conformance is claimed.

The necessary rationales are given in 7.2 for the PP refinements and in 7.3 for the PP additions.

9. Abbreviations

Abbreviation	Meaning
ACC	Agent Communication Channel
AE	Alter Ego
ADL	Agent Description Language
ADM	Administrator
AMS	Agent Management System
CA	Certification Authority
CC	Common Criteria
CRL	Certificate Revocation List
DF	Directory Facilitator
EAL	Evaluation Assurance Level
FIPA	Foundation for Intelligent Physical Agents
FSP	Functional Specification
HLD	High-Level-Design
JADL	JAVA Agent Description Language
JDK	Java Development Kit
JIAC	JAVA Intelligent Agent Componentware
JVM	JAVA Virtual Machine
LDAP	Lightweight Directory Access Protocol
PRNG	Pseudo Random Number Generator
SA	Security Agent
SAR	Security Assurance Requirements
SFR	Security Functional Requirements
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFR	TOE Security Functions Requirements
TSP	TOE Security Policy
USR	User

10. Glossary

Meaning
Agent: Agents are computer systems that are capable to act autonomous and flexible in a specified environment. The environment is implemented by a network of platforms. Mobile Agent, Service Agent, User Agent.
Agent Communication Channel (ACC): A part of the Agent Management System, which uses locally registered information about agents, to route messages between agents within the Agent Platform and to agents that reside on other Agent Platforms.
Agent Description Language (ADL): An ADL uses agent concepts as integral part of a programming language. There are many possible ways of designing ADLs, according to manifold programming paradigms.
Agent Migration: *Mobile Agents*
Agent Platform: An agent platform is the runtime environment for software agents. Similar to an operating system it provides services for the agents that are running on the platform.
Agent Management System (AMS): The AMS represents the main services by integrating agents into a run-time environment. Every agent acting on the local platform is registered by this agent. User defined agents can request information by the AMS about services or information about other user defined agents (yellow pages directory service). For reasons of trustworthiness each AMS possesses an asymmetrical key pair.
Alter Ego (AE): Through a user interface it is possible to use agent services. This user interface is communicating with the so called Alter-Ego agent, which translates the user intention into JADL.
Certificate: *X.509*
Certification Authority (CA): A third-party organization that issues digital certificates. A certificate is used in Public Key Infrastructure (PKI) to prove the identity of a sender to a recipient.
Certificate Revocation List (CRL): The CRL is a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reasons for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release.
Component: A *component* can always be part of *role* and can be seen as the part that realises the actual functionality.
Componentware: being built from a set of components respectively creating applications out of components. (JIAC: A JIAC agent is composed of a set of reusable components, which can be reconfigured and exchanged at run-time).
Directory Facilitator (DF): A Directory Facilitator (DF) is a service agent required by FIPA. Its purpose is to provide a yellow pages service to all agents of an agent society. Every time an agent is generated on (or moved to) a platform, it (should) register its services and when leaving a platform the agent should deregister its services.
Framework: comprehensive toolkit for developing and deploying agent systems covering a methodology, a programming language (JIAC: declarative agent definition language), a

Meaning
runtime environment (JIAC: component-based architecture with integrated management and security functionality, and a FIPA compliant infrastructure), supporting tools.
Foundation for Intelligent Physical Agents (FIPA): “FIPA is a non-profit organisation aimed at producing standards for the interoperation of heterogeneous software agents.” (www.fipa.org, 2003-02-21)
Group: A group interface specifies the internal handling on incoming messages from a role (interface of communication component) and handles speech-acts accordingly.
Human Service: Any human service directs the definition of a regular *Service* towards a service that is only usable by the Navigator/AE communication. Meaning that those services must be presented to a human user because they include a graphical user interface which the (human) user can operate.
JAVA Agent Description Language (JADL): JADL is used to define an agent’s knowledge in ontology to specify an action in a plan element, and to define a service through a service element.
JAVA Virtual Machine (JVM): The Java Virtual Machine (version 1.4.2_04) acts as an interpreter between the Java byte code and a computer's operating system. Using a Java Virtual Machine, you can run Java code on any number of different computer platforms, including Macintosh, Windows, and Unix.
Lightweight Directory Access Protocol (LDAP): Used to maintain directory databases.
Mobile Agent: Code and data of an agent are transferred to the remote platform; a specific start method will bring the agent back to life. That means the agent will always start at a specified point of execution (its initialization method).
Ontology: Ontology is used to describe knowledge of an agent. Ontology consists out of categories and functions. Categories specify data types and functions specify the possible actions combined with the listed types.
Plan Element: Plan elements are used to specify operations. Those operations are for example agent services and the service protocol itself.
Platform: Agent Platform
Role: *Typically a* role is a combination of *components, plan elements, services,* and *ontologies.* A realises an agent's functionality partial or in total. A set of roles can be combined to a *group.*
Runtime Environment: Agent Platform
Security Agent *(SA): The* SA provides a list of valid certificates (CL) and a certificate revocation list (CRL) that both were generated by a principal Certification Authority (CA). These certificates are including identification data (signed public keys) about trustworthy platforms and the associated public key. The certificates are signed by the CA.
Service: In JIAC a service is interpreted as an action that an agent fulfils for another. Services are initiated on the user side and directed towards the service provider. The service meta-protocol manages specific data conform to all services and supports the import of service specific protocols as enhancement.

Meaning
Service Agent: Agent services that serve human user needs are located stationary within the platform but outside the scope of the TOE. They do not provide any security functional components. In JIAC services are defined by plan elements expressed in JADL.
Speech Acts: Speech Acts are used when agents talk to each other, internal on the same platform via the Java Virtual Machine or when talking to a remote platform by the Agent Management System.
User Agent: Service Agent
X.509: X.509 *is a* format for certified Public Key's, which are suitable for use in various Public Key Infrastructure systems. These certificates are useful for encrypting messages using Privacy Enhanced Mail and forming SSL network connections (HTTPS). The X.509 certificates as provided by the Certification Authority are used to establish a network of trust between agent platforms.

11. Bibliography

Criteria:

[1] Common Criteria, Part 1: Introduction and general model, August 1999, Version 2.1, CCIMB-99-031, Incorporated with interpretations as of 2002

[2] Common Criteria, Part 2: Security functional requirements, August 1999, Version 2.1, CCIMB-99-032, Incorporated with interpretations as of 2002

[3] Common Criteria, Part 3: Security assurance requirements, August 1999, Version 2.1, CCIMB-99-033, Incorporated with interpretations as of 2002

Methodology:

[4] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999, Incorporated with interpretations as of 2002.02.28

Laws, Regulations:

[5] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001 (BGBI. I S.876 ff)

[6] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) vom 16.November 2001 (BGBl. I S. 3074ff)

[7] Geeignete Kryptoalgorithmen: In Erfüllung der Anforderungen nach §17 (1) SigG vom 22. Mai 2001 in Verbindung mit Anlage 1, I 2, SigV vom 22. November 2001, Entwurf vom 15.04.2002

[8] Anwendungshinweise und Interpretationen zum Schema, AIS20, Version 1, 02.12.1999, Bundesamt für Sicherheit in der Informationstechnik

Standards:

[9] U.S. DEPARTMENT OF COMMERCE Technology Administration National Institute of Standards and Technology: FIPS PUB 180-1, Secure Hash Standard, 1995 April 17

[10] Data Encryption Standard (DES), FIBS PUB 46-3, US NBS, 1977, reaffirmed 1999 October 25, Washington

[11] RSA Laboratories, PKCS #1: RSA Encryption Standard, An RSA Laboratories Technical Note Version 1.5, Revised November 1, 1993

[12] CryptoBytes Vol. 3, Number 1 - spring 1997, RSA Laboratories, The technical newsletter of RSA Laboratories, a division of RSA Data Security, page 9

Company Internals:

[13] Configuration list of the JIAC IV project, JIAC-IV_Cert_Configuration_List.txt, Version 0.3, released November 21st, 2003 (relevant to version JIAC-IV_Cert_4_3_1)