FOUNDATION FOR INTELLIGENT PHYSICAL AGENTS

FIPA Security Work Group Request For Information (RFI)

Document title	FIPA Security Work Group Request For Information (RFI)		
Document number	f-out-00065 version2	**Document source**	FIPA Security WG
Document status	Preliminary	**Date of this status**	2001/06/14
Submissions due by	2001/07/17		
Contact	security@fipa.org		
Change history			
2000/10/20	Initial draft		
2001/02/02	Final version submitted as a first request for information		
2001/04	First RFI Issued		
2001/05/29	Initial draft of the second request for information to be submitted to FIPA by the 2001/05/30		
2001/06/14	New version of RFI for 2nd call completed		
2001/06	2nd RFI issued		

Geneva, Switzerland

Notice

Use of the technologies described in FIPA's specifications may infringe patents, copyrights or other intellectual property rights of FIPA Members and non-members. Nothing in this document should be construed as granting permission to use any of the technologies described. Anyone planning to make use of technology covered by the intellectual property rights of others should first obtain permission from the holder(s) of the rights. FIPA strongly encourages anyone implementing any part of FIPA's specification to determine first whether part(s) sought to be implemented are covered by the intellectual property of others, and, if so, to obtain appropriate licenses or other permission from the holder(s) of such intellectual property prior to implementation. This document is subject to change without notice. Neither FIPA nor any of its Members accept any responsibility whatsoever for damages or liability, direct or consequential, which may result from the use of FIPA's specifications.

Foreword

The Foundation for Intelligent Physical Agents (FIPA) is an international organization that is dedicated to promoting the industry of intelligent agents by openly developing specifications supporting interoperability among agents and agent-based applications. This occurs through open collaboration among its member organizations, which are companies and universities that are active in the field of agents. FIPA makes the results of its activities available to all interested parties and intends to contribute its results to the appropriate formal standards bodies.

The members of FIPA are individually and collectively committed to open competition in the development of agent-based applications, services and equipment. Membership in FIPA is open to any corporation and individual firm, partnership, governmental body or international organization without restriction. In particular, members are not bound to implement or use specific agent-based standards, recommendations and FIPA specifications by virtue of their participation in FIPA.

The FIPA specifications are developed through direct involvement of the FIPA membership. The status of a specification can be either Preliminary, Experimental, Standard, Deprecated or Obsolete. More detail about the process of specification may be found in the FIPA Procedures for Technical Work. A complete overview of the FIPA specifications and their current status may be found in the FIPA List of Specifications. A list of terms and abbreviations used in the FIPA specifications may be found in the FIPA Glossary.

FIPA is a non-profit association registered in Geneva, Switzerland. As of January 2000, the 56 members of FIPA represented 17 countries worldwide. Further information about FIPA as an organization, membership information, FIPA specifications and upcoming meetings may be found at http://www.fipa.org/.

Contents

1 Glossary

1.1 Abbreviations

Abbreviation	Expansion
ACC	Agent Communication Channel
ACL	Agent Communication Language
AMS	Agent Management System
AP	Agent Platform
CCL	Common Command Language
CL	Content Language
DF	Directory Facilitator
FAB	FIPA Architecture Board
FIPA	Foundation for Intelligent Physical Agents
GUID	Globally Unique Agent Name
MTP	Message Transport Protocol
MTS	Message Transport Service
(FIPA) TC	(FIPA) Technical Committee
(FIPA) WG	(FIPA) Working Group
RFI	Request For Information

1.2 Definitions

Action
A basic construct that represents some activity, which an agent may perform. A special class of actions is the communicative acts.

Agent
An agent is the fundamental actor in a domain. It combines one or more service capabilities into a unified and integrated execution model that can include access to external software, human users and communication facilities.

Agent Communication Language
A language with precisely defined syntax, semantics and pragmatics that is the basis of communication between independently designed and developed software agents.

Agent Communication Channel
A part of the Agent Platform which uses information provided by the Agent Management System to route messages between agents within the Agent Platform and to agents that reside on other Agent Platforms.

Agent Management System
A part of the Agent Platform which manages the creation, deletion, suspension, resumption, authentication and migration of agents on the Agent Platform and provides a white pages directory service for all agents resident on an Agent Platform.

Agent Platform
Provides an infrastructure in which agents can be deployed. An agent must be registered on a platform in order to interact with other agents on that Agent Platform or indeed other Agent Platforms. An Agent Platform consists of three capability sets: An Agent Communication Channel, an Agent Management System and at least one Directory Facilitator.

Communicative Act
A special class of actions that correspond to the basic building blocks of dialogue between agents. A communicative act has a well-defined, declarative meaning independent of the content of any given act. Communicate acts are modelled on speech act theory.

Content
That part of a communicative act which represents the domain dependent component of the communication. Note that "the content of a message" does not refer to "everything within the message, including the delimiters", as it does in some languages, but rather specifically to the domain specific component. In the Agent Communication Language semantic model, a content expression may be composed from propositions, actions or Identifying Referring Expressions.

Content Language
The content of a FIPA message refers to whatever the communicative act applies. If, in general terms, the communicative act is considered as a sentence, then the content is the grammatical object of the sentence. This content can be encoded in any language, called the content language.

Conversation
An ongoing sequence of communicative acts exchanged between two (or more) agents relating to some ongoing topic of discourse. A conversation may (perhaps implicitly) accumulate context that is used to determine the meaning of later messages in the conversation.

Directory Facilitator
A part of the Agent Platform that provides a yellow pages directory service for agents. It stores descriptions of the agents and the services they offer.

Interaction Protocol
A common pattern of conversations used to perform some generally useful task. An interaction protocol is often used to facilitate a simplification of the computational machinery needed to support a given dialogue task between two agents.

Message
An individual unit of communication between two or more agents. A message corresponds to a communicative act, in the sense that a message encodes the communicative act for reliable transmission between agents. Note that communicative acts can be recursively composed, so while the outermost act is directly encoded by the message, taken as a whole a given message may represent multiple individual communicative acts.

Message Content
See *Content*.

Message Transport Protocol
An instance of a network transport protocol that is used to carry out the physical transfer of messages between two Agent Communication Channels, between an agent and a remote or local Agent Communication Channel, or between two agents.

Message Transport Service
A service provided by the Agent Platform to which the agent is attached. The Message Transport Service supports the transportation of Agent Communication Language messages between agents. On any given Agent Platform, the Message Transport Service is provided by the Agent Communication Channel.

Ontology
An explicit specification of the structure of a certain domain (for example, e-commerce, sport, etc.). For the practical goals of FIPA (that is enabling development and deployment of inter-operable agent-based applications), this includes a vocabulary (that is, a list of logical constants and predicate symbols) for referring to the subject area and a set of logical statements expressing the constraints existing in the domain and restricting the interpretation of the vocabulary. Ontologies therefore provide a vocabulary for representing and communicating knowledge about some topic and a set of relationships and properties that hold for the entities denoted by that vocabulary.

Ontology Name
The ontologies referred to by agents that can be provided by different ontology servers. Consequently, these ontology names are constructed from the ontology agent name and the ontology logical name (given by the ontology designer, for example, "car").

2 Objectives

The main objective of this Request For Information is to obtain information, which will allow FIPA to help establish new work plans for future FIPA activities in the area of Multi-Agent System security.

Submissions shall focus on security mechanisms to implement security policies and the policies and requirements that constrain those mechanisms. Submissions, in the form of technology artefacts (including but not limited to specifications, source code and products), shall address one or more of the following areas:

1 A definition and architecture outlining what constitutes a secure multi-agent architecture, e.g. what are the categories and/or policies that define the security features of a multi-agent system?

2 Definition of the minimum set of security concepts within a multi-agent architecture that provides the minimum conditions of what it is to be a secure multi-agent architecture. In more detail, this includes:

   2.1 Access by an agent to other agents representing platform or infrastructure services, service users, domain specific service providers and mediators.

   2.2 The security of agent message transport services.

   2.3 The security of agent directory services.

   2.4 Security aspects of FIPA-ACL messages

   2.5 Security-related conversational interactions between agents.

   2.6 Issues of identity and authentication related to agents.

3 Criteria for classifying the degree of security within a multi-agent architecture. For instance, if an architecture supports *category-1* trust features, it implements or supports encryption of messages that follow a standard and may include financial payment security method. C*ategory-2* may be a protocol that identifies and authenticates an agent, platform or other related service (e.g., configuration boot-up for small devices onto a network when they are launched etc.). Using such types of definitions, can we determine how secure an architecture is (within a certain limit of risk)?

4 The definition of aspects of classic and agent-based security requirements that provide partial solutions to semantic attacks.

5 An analysis of security problems which occur in multi-agent architectures which support general agent concepts of autonomy, reactivity, mobility, rich communication protocols and how these problems can be handled, e.g. different types of verification via know agents, employing social concepts of trust etc.

6 An analysis of the possible types of security policies that should exist within architecture and how these policies relate to social concepts of trust. Can these types of policies be mapped to concepts of domains and policies within the abstract architecture in FIPA [FIPA0001]?

7 Defining the possible ontological models of security and trust within multi-agent systems that enable verification of a system. Does this require new communication protocols, semantics and channels? What is the impact of considering these concepts on current FIPA and / or FIPA type multi-agent systems?

8 An analysis and evaluation of how social and organisational concepts of trust can bring different types of solutions to security concerns within multi-agent systems.

9 Other related areas such as issues of trust, ownership, authority transfer, etc.

3 Introduction

Agent oriented applications and agent-based systems are increasingly demanding security guarantees that concern confidentiality, integrity, availability, accounting and non-repudiation in order to be deployed in application domains such as e-commerce and e-business in general.

The main security needs may be complicated by the specific properties of agents and agent systems, such as the distributed and open characteristics of agent-based applications, the inherent social interactivity of agents, and the fact that agents may act autonomously while at the same time representing some user or other principal.

Issues of security, including privacy, data integrity, authentication and authorization, non-repudiation and trust have been widely studied over thousands of years, and a wide range of technological, social, and legal solutions have been developed. In computer systems, particularly distributed systems, existing mechanisms and policies have been augmented by new techniques based on the computational and communicative power available to their designers. These new mechanisms, while powerful, are still subject to social and legal validation and acceptance, and much of this is based on familiarity and comprehensibility. This explains in part why powerful computer-based security mechanisms such as PKI (public key infrastructure) have only been accepted slowly, and why most security is still based on simple password schemes.

For these reasons, it is particularly important that any organization which is embarking on security-related work should solicit input from experts and those with experience in this or a related field, and should ensure that its work is not at odds with mainstream security developments. In the field of intelligent multi-agent systems, this is even more important: imbuing software agents with the power to plan and act autonomously requires that the designers and users of these systems can trust the agents to behave appropriately.

FIPA is therefore issuing a RFI, or Request For Information, in which individuals and organizations with expertise in computer system security and multi-agent systems are invited to propose solutions to some or all of the specific problems associated with the security of agent systems. In section 6 below we set forth the specific issues which we wish to address, together with a series of scenarios which demonstrate how these issues, individually or collectively, apply to particular multi-agent applications.

Submissions can address all or some of the issues listed below. A submission should indicate which specific issue or issues are being addressed. We also invite submitters to comment on the relevance of their submission to particular scenarios, and to offer additional scenarios, which they believe that FIPA should consider.

4 Instructions for Submitters

4.1 Responding to this RFI

4.1.1 Timescales

See *Table 3* in *Section 6.11, Timetable* for submission deadlines.

4.1.2 Notification of Intent

Individuals or companies must notify the FIPA secretariat (**secretariat@fipa.org**) of their intention to respond to this RFI.

4.1.3 Separate Proposals

A submitter may respond to any or all parts of this RFI. Each response will be evaluated independently by the Security WG. It should be noted that a given response, theoretical or tested and proven work, may support two or more parts of the RFI.

4.1.4 Completeness of Proposals

Proposals for each separate response item need not be complete. However, reasons for not being complete must be clearly stated.

Outlines and short summaries of intended submissions are welcome at any stage in order to get early feedback from the FIPA security WG (email security-chair@fipa.org). In addition these can be submitted to the security email list. security@fipa.org.

4.2 Confidential and Proprietary Information

The FIPA specification adoption process is an open process. Responses to this RFI become public documents of the FIPA and are available to members and non-members alike for perusal. No confidentiality or proprietary information of any kind will be accepted in a submission to this RFI.

4.3 Format of RFI Submissions

This section provides guidance on how to structure a submission.

4.3.1 General

- Submissions must be written in English.
- Submissions should be concise and easy to read.
- Submitted documentation should be directly relevant to the technology requested in the RFI.
- The file format of the submissions should be one of plain text, HTML, PDF, Microsoft Word or PostScript.

4.3.2 Suggested Outline

A two-part structure for a submission is suggested:

PART I

- Submission contact point, including name, postal address, affiliation, email address, telephone number, fax number.

- Completeness of the submission (see Section *4.1.4, Completeness of Proposals*).

- Overview of the submission.

PART II

- Proposed specification(s).

4.4 How to Submit

Submitters should send an electronic version of their submission to the FIPA Secretariat (secretariat@fipa.org) and a copy to the Security WG mailing list (**security@fipa.org**).

4.5 Response to Submissions

Feedback on submissions will be provided in accordance with the timescales shown in *Table 3*. The response will be send to the email and postal address provided by the submitter.

5 General Requirements for Submissions

Proposals should not conflict with the FIPA specifications given in *Table 1* and *Table 2*.

Note the following when writing a proposal:

- Any conflicts must be clearly identified, along with reasons for them.
- Emphasis should be put on the use of reusable components.
- Proposals shall preserve maximum implementation flexibility and interoperability.
- The use of UML modelling is desirable, but not mandatory.
- Proposals can be based on theoretical work or tested, proven work.
- Proposals shall indicate the current status of the work such as theoretical, simulation, experimental, limited trials, field trials.
- Proposals should indicate which of the problems areas identified in Section 2 that they are attempting to address.

6 Specific focus for proposals

Proposals shall describe solutions that cover security issues at one or more of the following:

- Agent service level (e.g., transport service [FIPA00067], discovery or directory service [FIPA00023]).
- Agent communication level (i.e., ACL).
- Conversational level (e.g., negotiation of secure behaviour, etc.).

Before examining each of these, we consider the state of existing and previous FIPA specifications in this area.

6.1 Current FIPA ACL security specification and limitations

Currently, ACL messages sent by agents are wrapped in an "envelope" for transport [FIPA00067]. This envelope or transport header contains an encryption field for encrypting the ACL message. But the loose specification of the encryption field will mean that it will be very difficult for sender and receiver to explicitly agree a common encryption scheme. The ACL or envelope or interactions protocols or ontology contain no support for verifiable authentication or authorisation. A general overview of agent security is also covered in an appendix of the FIPA Abstract Architecture, see section 6.3.

6.2 Previous FIPA ACL security specification and limitations

Authentication was defined by a previous FIPA management specification (see [FIPA00002] which is now Obsolete) in terms of:

- Signature field for the AMS description.
- an authority parameter in the `ap-description` frame.

Message privacy and integrity and key management is defined as follows (see [FIPA00020] which is Obsolete):

- The Type of message privacy, integrity and key management is specified using fields in the ACL envelope sender address field.
- Public keys are stored in the DF.
- Private keys are stored in the AMS.
- Public and private key pairs (PKI) are used for bulk ACL message encryption.
- Message privacy is defined on a per message basis by the sender.

There are several major limitations to the current specifications:

- DF cannot authenticate DF directory write access by other agents (no signature in the DF description).
- Public keys are stored in the DF - but not all agents are service providers and register with the DF.
- The platform security policy seems to be specified solely in terms of a certificate authority.
- Private keys are distributed to the AMS.
- Public and private key pairs (PKI) are used for bulk ACL message encryption.

- Message privacy cannot be defined as part of a general platform security policy, i.e., sender rather than the platform decides the degree of message privacy.

- Different levels of security can be requested by the sender, these can violate the agent platform's security policy as a whole.

For a more detailed analysis of the limitations of the current specifications see [1].

6.3 Problem areas

6.3.1 Agent Platform Services

Historically, FIPA specifications described agent platform services in terms of interactions with a collection of agents which together comprised a platform [FIPA00023]. More recently, FIPA has developed the Abstract Architecture specification [FIPA00001] that defines a set of abstract services and objects to support agent registration, discovery, and message exchange. These abstractions may be realized in terms of a number of different concrete technologies, such as Java, CORBA, COM, and so forth.

The Abstract Architecture is almost silent on the question of security. In the message transport service, there is a notion of "quality of service" which is presumed to extend to qualities such as message integrity, data privacy (encryption), non-repudiation, and so forth. In the discovery or directory service, there is the notion that certain operations may fail due to insufficient privilege or permission.

FIPA is interested in submissions that address security aspects of agent communication and discovery services as described in the FIPA Abstract Architecture [FIPA00001]. Among the detailed issues that should be addressed are:

- Access control policies and mechanisms used by agents representing platform or infrastructure services, service users, domain specific service providers and mediators

- Security policies and mechanisms associated with message transport including message integrity, message privacy, non-repudiation schemes

- Security issues associated with discovery services, including access control associated with individual directory entries

- Agent description elements – standardized attributes – associated with security. (Some of these may also be embedded in transport descriptors, which appear in agent descriptions.)

For end-to-end interoperation between agents based on different platforms or technologies, the Abstract Architecture [FIPA00001] requires that agent names be opaque at the ACL level and above, and that gateways provide robust bi-directional mappings between different encodings of names. For some applications, it may be important that agent names be unforgeable, or that it be possible to determine the authority which created the name. For many applications it may be necessary to also securely bind the name to some additional attribute list such as a vendor name and address or to an access control list. FIPA is interested in submissions that explore the issues of secure agent naming, including digitally signed names and name management services.

6.3.2 ACL Messages

What are the security issues associated with ACL messages? Some of the issues concern how the security should be specified such that the agent can ascertain and reason about the level of security is and what level of security is needed. How can the agent dynamically configure the type and level of security? Security issues may also include developing standardized ontologies and adding fields such as the level of encryption or a signed digital certificate into the MTS transport envelope or ACL message.

6.3.3 Conversational Interactions

Is there utility in developing standardized interaction protocols and ontologies associated with security? Such standardization may enhance the usability of non-repudiation message transport schemes, as it allows a trusted third party to verify security-related interactions without having to be cognizant of application-specific interaction protocols and ontologies.

6.3.4 Identity

Issues of identity arise at all levels – message transport, access control, agent description, ACL, and interaction protocols.

6.4 Scenarios

In this section, we present a series of simple security-related scenarios to illustrate some of the pertinent issues:

- Publisher/directory scenario.
- Courier/broker scenario.
- Task Allocation scenario.
- Multi-domain operation scenario.

6.4.1 Publisher/Directory Scenario

Let assume that we have 5 agents:

- Agent A wants to buy fruits and ice cream.
- Agent B sells fruits.
- Agent C sells ice cream.
- Agent D is a malicious agent.
- FIPA DF agent acts as a directory/publisher for services by different vendors, see [FIPA00023]. All directory entries are in DF agent directories are public.

Agent B and C register their services, i.e., “selling fruits” and “selling ice cream”, with a Directory Service, e.g., DF. Given the current FIPA specifications, agent D can:

1. Pretend to be agent C and change C’s service description at the DF, declaring that C now sells wine instead of ice cream. In this way agent C will not be able to make any profit since it will be asked to provide a service that it is not able to support and nobody will ask it for the real service it is able to provide.
2. Pretend to be agent A and places and order with agent B for a 100 kG of plums. Therefore, agent B sends 100 kG of plums and the bill to agent A. Who is going to pay the bill? What about the plums?
3. Pretend to be agent B and gets paid that for providing a service that it does not intend to honour.
4. Pretend to be a multitude of customers and overload B and C with a deluge of fake offers to be processed resulting in valid service offers becoming delayed and perhaps causing them to be subsequently withdrawn.

In this scenario, the direct security concerns are:

- Lack of authentication: an agent can masquerade as another agent (list items 1-3)

The secondary security concerns are:

- Authorisation problems/lack of access of control:
  - a masquerading agent is authorised to change another agent's published service description (1)
  - any agent can also read any service provider agent's entry in the DF
- Service Disruption: a masquerading agent can change another agent's published service description thereby disrupting the normal service provision of that agent (2)
- Denial of Service Attack (4).

6.4.2 Courier/Broker Scenario

Let assume that we have three agents:

- Agent A is a consumer.
- Agent B is a vendor.
- A courier agent (broker) agent acts as an intermediary for all messages between the seller and the buyer.

If all discourse between A and B is via the courier agent, the following security related problems could occur:

1. The courier agent can open up messages between A and B and observe their contents
2. The courier agent can modify the messages between A and B
3. The courier agent can insert messages from other parties to masquerade as A or B. For example if the courier was an estate agent (broker that sells houses), it could hypothetically say "A has pulled out of a deal to buy the house", thus putting pressure on B to possibly sell at a lower-price.
4. Agent A can deny having sent a message, the courier can deny having been called to deliver it, agent B can deny having received a sent message.

In this scenario, the main security concerns are:

- Lack of privacy: the courier agent can open up and see the contents of messages between A and B (1).
- Lack of integrity: the estate agent can misrepresent or corrupt messages between A and B (2).
- Lack of authentication: an agent can masquerade as another agent (3).
- Repudiation: an agent can deny that an event such as a message transmission or message delivery has occurred (4).

Brokerage is discussed in more detailed in [FIPA00033].

6.4.3 Task Allocation Scenario

In the contract net protocol (see [FIPA00029]) one agent takes the role of *manager*. The manager wishes to have some task performed by one or more other agents, and further wishes to optimize a function that characterizes the task. This characteristic is commonly expressed as the *price*, in some domain specific way, but could also be soonest time to completion, fair distribution of tasks, etc.

The manager solicits *proposals* from other agents that specifies the task and any conditions the manager is placing upon the execution of the task. Agents receiving the call for proposals are viewed as potential *contractors*, and are able to generate proposals to perform the task. They may also be able to sub-contract the task to another contractors, behaving as a mnager in this level of interaction. The contractor's proposal includes the preconditions that the contractor is setting out for the task, which may be the price, time when the task will be done, etc. Alternatively, the contractor may *refuse* to propose. Once the manager receives back replies from all of the contractors, it evaluates the proposals and makes its choice of which agents will perform the task. One, several, or no agents may be chosen. The agents of the selected proposal(s) will be sent an acceptance message, the others will receive a notice of rejection. The proposals are assumed to be binding on the contractor, so that once the manager accepts the proposal the contractor acquires a commitment to perform the task. Once the contractor has completed the task, it sends a completion message to the manager.

For the interaction between the manager and the contractor agents, the following security related problems could occur:

1. The proposals can be modified by either the contractor or the manager.

2. The rejected contractors can deny having received a rejection instead of an acceptance.

3. The manager could divulge information to contractors that it does not want in turn divulged to sub-contractors.

4. A manager cannot prevent a contractor from modifying any details of the contract when it is passed on to a sub-contractor.

In this scenario, the main security concerns are:

- Lack of integrity: a manager or contractor can misrepresent or corrupt messages (1).

- Non-repudiation: the manager or contractor can deny that an event such as a message transmission or message delivery has occurred or introduce a spurious event such as an unsubstantiated message (2).

- Lack of authority delegation: an agent such as a manager cannot control how second parties protect confidential information on to third parties (3-4).

6.4.4 Multi-domain operation scenario

Agents operating within one domain may require access to interoperate with agents in a different domain. For example, consider a travel service [FIPA00080], a travel broker can access and use many different types of travel services such as flight reservation services, hotel room reservation systems, train travel reservation services, travel insurance service and so on. Some of these services are location specific such as the train travel while others may be global such as the airline reservation. Rather than model this (travel assistance service) as a single domain, we can model this as a set of geographical and application specific domains that may interoperate, e.g., travel service domains such as flight-reservation, UK-train-reservation-service, London-taxi-reservation and travel insurance for UK-residents. We consider how services in these different domains can be set-up interact.

Let's assume, a travel broker is already registered to operate flight reservation services (for example it is a member of IATA). We can say it is trusted to operate a flight reservation service. Let's consider how it interoperates and how it becomes trusted to operate train reservation services. Within the UK-train-reservation domain, there are several services that a broker would need to use such as a national UK directory services that gives information about train timetables and fares. However, to book train travel, there is no UK wide train seat reservation service, one must book with individual train line operators. How does a service trusted to operate in one domain become trusted to operate in a new domain? What security threats and trust abuses can occur?

There are at least two basic "bootstrapping" patterns to describe how an agent that is trusted in one domain becomes trusted in another domain: there is an inter-domain agreement or each agent must register and elevate itself to become trusted in each domain it operates in. This requires information about the trustworthiness in one domain to be transferred to another domain. For example, because the travel broker is licensed or registered to operate in the airline reservation domain, there is an inter-domain agreement that allows it to operate as a fully-fledged train reservation service provider without having to authenticate itself to its peers and the establishment in the new domain. There are several problems that can occur.

- Providers may try to mask a loss of status in one domain, such as a downgrade in financial status, in another domain.
- The transfer of an agent's identity and trustworthiness information between domains may get be falsified

6.5 Relationship to Existing FIPA Specifications

Table 1 and *Table 2* identify existing FIPA Specifications that have a relationship to technologies requested in this RFI. All the specifications can be retrieved from http://www.fipa.org/specs/.

Specification Number	Title
FIPA00001	FIPA Abstract Architecture Specification
FIPA00023	FIPA Agent Management Specification
FIPA00029	FIPA Contract Net Interaction Protocol
FIPA00033	FIPA Brokering Interaction Protocol
FIPA00067	FIPA Agent Message Transport Service Specification
FIPA00080	FIPA Personal travel Assistance Specification

Table 1: Referenced Relevant FIPA Specifications

Specification Number	Title
FIPA00037	FIPA Communicative Act Library Specification

Table 2: Non-Referenced Relevant FIPA Specifications

6.6 Related Non-FIPA Documents

[1] Poslad S and Calisti M. Towards improved trust and security in FIPA agent platforms. Autonomous Agents 2000 Workshop on Deception, fraud, and trust in agent societies, Barcelona, June 2000.

[2] Poslad S, Charlton P and Calisti M. Protecting What Your Agent Is Doing. (to appear in the AgentLink Newsletter No.7, available from http://www.agentlink.org/newsletter/).

6.7 Mandatory Requirements

None.

6.8 Optional Requirements

None.

6.9 Issues to be Discussed

Proposals should discuss potential impact on FIPA specifications. In particular, proposals should discuss interrelationship with FIPA ACL specs, FIPA Architecture specs.

6.10 Other Information

None.

6.11 Timetable

The timetable for this RFI is given in *Table 3*. Note that FIPA may, in certain circumstances, extend deadlines while the RFI is running, or may elect to have more than one revised submission step.

Action	**Latest Date**
Electronic receipt of material	2001-07-17
Acknowledgement of submission	2001-07-20
FIPA Security WG reviews submissions in Sendai (Japan)	2001-07-23

Table 3: Timescales

These deadlines are for the 2nd phase of submissions. Please contact the security@fipa.org for information about the next phase of submissions.