- FOUNDATION FOR INTELLIGENT PHYSICAL AGENTS

# **5** FIPA Nomadic Application Support Specification

Document title	FIPA Nomadic Application Support Specification			
Document number	XC00014D	Document source	FIPA Nomadic Application Support TC	
Document status	Experimental	Date of this status	2001/08/10	
Supersedes	FIPA00062, FIPA00063, FIF	PA00065, FIPA00066		
Contact	fab@fipa.org			
Change history				
2000/09/28	Approved for Experimental			
2001/08/10	Line numbering added			

16 © 2000 Foundation for Intelligent Physical Agents - http://www.fipa.org/

#### 17 Geneva, Switzerland

#### Notice

Use of the technologies described in this specification may infringe patents, copyrights or other intellectual property rights of FIPA Members and non-members. Nothing in this specification 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 this 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 specification 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 this specification.

#### 18 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 agentbased 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 agentbased 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/.

38	1	Scope	)	1
39	2	Gene	ral Analysis	2
40	2	2.1 C	Dverview	2
41	2	2.2 N	Ionitoring and Controlling Quality of Service	3
42	2	2.3 N	legotiation of Message Transport Requirements	4
43		2.3.1	Negotiation About Message Transport Protocols	4
44		2.3.2	Negotiation About Message Representation	4
45	3	Noma	dic Application Support Ontology	5
46	3	8.1 C	bject Descriptions	5
47		3.1.1	Quality of Service Description	5
48		3.1.2	Rate Value	6
49		3.1.3	Time Value	7
50		3.1.4	Probability Value	7
51		3.1.5	Change Constraint	8
52		3.1.6	Time Constraint	8
53		3.1.7	Communication Channel Description	8
54		3.1.8	Transport Protocol Description	9
55		3.1.9	Transport Protocol Selection	9
56		3.1.10	Message Representation Description	9
57		3.1.1	Message Representation Selection	10
58	3	8.2 F	unction and Predicate Descriptions	11
59		3.2.1	Request Monitoring Information	11
60		3.2.2	Subscribe to Changes	12
61		3.2.3	Open Communication Channel	12
62		3.2.4	Close Communication Channel	12
63		3.2.5	Activate a Message Transport Protocol	
64		3.2.6	Deactivate a Message Transport Protocol	13
65		3.2.7	Select a Message Transport Protocol	13
66	3	8.3 E	xceptions	
67		3.3.1	Not Understood Exception Propositions	13
68		3.3.2	Refusal Exception Propositions	
69		3.3.3	Failure Exception Propositions	14
70	4	Regis	tration of the Control Agent and Monitor Agent with the DF	
71	5	-	arios	
72	5	5.1 F	egistration with a DF	16
73	5	5.2 N	legotiating Message Transport Protocols	17
74	5		legotiating Message Representations	
75	5		lessage Exchange Over a WAP Message Transport Protocol	
76		5.4.1	Message Exchange Activation by an Agent in a Mobile Host	
77		5.4.2	Message Exchange Termination to an Agent in a Mobile Host	
78	6	Inforn	native Annex A — Paramedic Scenario	
79	6		Dverview	
80	6		eamless Roaming	
81		6.2.1	Disconnection and Reconnection of an Message Transport Connection	
82		6.2.2	Example Negotiation of a Message Transport Protocol	
83		6.2.3	Example Negotiation of a Message Representation	
84	7		ences	
85				

# 85 **1 Scope**

This document is part of the FIPA specifications and deals with agent middleware to support applications in nomadic environment. The environment of mobile computing is very different compared to today's environment of traditional distributed systems in many respects. Bandwidth, latency, delay, error rate, interference, interoperability, computing power, quality of display, among other things may change dramatically as a nomadic end-user moves from one location to another. All these cause new demands for adaptability of data services.

Adaptability to the changes in the environment of nomadic end-users is an important issue. A nomadic end-user confronted with these circumstances would benefit from having the following functionality provided by the infrastructure: information about expected performance, agents controlling over the transfer operations, a condition-based control policy, capability provided by agents to work in a disconnected mode, advanced error recovery methods, and adaptability.

- 98 This specification gives an overview of the Nomadic Application Support area and contains specifications for:
- 100 Monitor Agent (MA) functionality,
- 102 Control Agent (CA) functionality, and,
- 104 An ontology for representing the quality of service of the Message Transport Service in the context of nomadic 105 application support.
- In addition, two other FIPA specifications are related to Nomadic Application Support: FIPA Agent Message Transport
   Protocol for WAP Specification [FIPA00076] and FIPA ACL Message Representation in Bit-Efficient Encoding
   Specification [FIPA00069].
- 110

91

97

99

101

103

## 111 2 General Analysis

#### 112 **2.1 Overview**

113 The results of current developments in both wireless data communications and mobile computers are being combined 114 to facilitate a new trend: nomadic computing. Compared to today's traditional distributed systems, the nomadic 115 computing environment is very different in many respects. Bandwidth, latency, delay, error rate, quality of display and 116 other non-functional parameters may change dramatically when a nomadic end-user moves from one location to 117 another and thus from one computing environment to another, for example, from a wireline LAN to a UMTS network. 118 The variety of mobile workstations, handheld devices and smart phones, which allow nomadic end-users to access 119 Internet services, is increasing rapidly. The capabilities of mobile devices range from very low performance equipment 120 (such as PDAs) up to high performance laptop PCs. All these devices create new demands for adaptability of Internet 121 services. For example, PDAs cannot display properly high quality images and as nomadic end-users may be charged 122 based on the amount of data transmitted over the GPRS-UMTS network, they may have to pay for bits that are totally 123 useless to them.

124

128

125 Confronted with these circumstances, the nomadic end-user would benefit from having the following functionality 126 provided by the infrastructure: information about expected performance, agent monitoring and controlling the transfer 127 operations, and adaptability.

The ability to automatically adjust to changes in a transparent and integrated fashion is essential for *nomadicity*; nomadic end-users are usually professionals in areas other than computing. Furthermore, today's mobile computer systems are already very complex to use as productivity tools. Thus, nomadic end-users need all the support that a FIPA agent-based distributed system can deliver and adaptability to the changes in the environment of nomadic endusers is an important issue.

134

147

149

155

157

FIPA uses the Wireless Application Protocol (WAP) [WAP99] as its wireless Message Transport Protocol (MTP - see [FIPA00076]). The WAP Forum has developed industry-wide specifications for low bandwidth wireless services (such as GSM, GPRS, etc.) and wireless devices (such as mobile telephones and personal digital assistants). The WAP specification address the characteristics of wireless networks by adapting low bandwidth wireless services and low-end mobile devices to the special requirements of information services. The WAP specification defines a set of standard components that can be used in agent message communication, such as standard data formats and standard data communication protocols.

The adaptation of applications to various nomadic computing environments is an important area. There are several
 tasks that agents need to carry out during application adaptation:

- 146 1. Selection of MTP and Message Transport Connection (MTC) to be used for agent communication.
- 148 2. Selection of an ACL and content language representation to be used for agent communication.
- Provision of support for application agents to carry out adaptation of application data, such as still images, video and audio, XML, etc. Today's Internet application data (such as multimedia content) are designed with high performance desktop PCs and high quality displays in mind. Therefore, the application data is frequently unsuitable for nomadic computing using wireless wide-area networks and low performance mobile devices, and hence requires modification.
- 156 4. Communication between agents performing adaptation.
- 158 The FIPA Nomadic Application Support specifications define agent middleware to:
- 159
- 160 Monitor and control an MTP and the underlying MTC, and, 161
- An ontology for representing the quality of service of the Message Transport Service in the context of nomadic application support.

- 164 In addition, this specification gives examples of the use of the above scenarios.
- 165

174

176

178

180

182

184

#### 166 2.2 Monitoring and Controlling Quality of Service

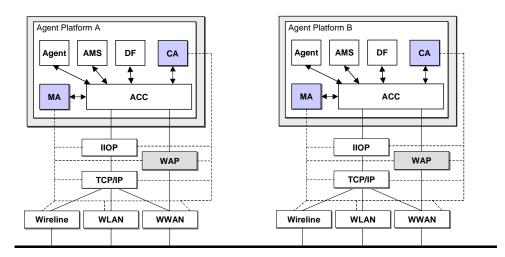
The functions required to carry out monitoring and controlling for quality of service can be split into several specific
 tasks:

- 170 1. Observing the quality of service of MTPs and MTCs,
- Measuring (if there are no other means to obtain the required information) the quality of service of an MTP and MTC,
- 175 3. Collecting information from the observing and measuring sources,
- 177 4. Analysing the information, and,
- 179 5. Controlling an MTC and selecting an MTP.

181 Based on this division, the agent middleware consists of the following logical agents (see *Figure 1*):

183 A Monitor Agent (MA) which carries out tasks 1 through 4, and,

- 185 A Control Agent (CA) which carries out task 5.
- 186



- 187 188
- 100

189

190

196 197

198

200 201 Figure 1: Reference Model of Agent based Adaptation

The most appropriate configuration of MAs and CAs is that there is at least one pair in each AP involving adaptation. The MA may measure the actual quality of service of an MTC, if the network running an MTC does not provide users with required performance data<sup>1</sup>.

195 An MA may:

- Consist of network-service-specific components that collect raw performance data at fixed intervals,
- 199 Provide a repository for the measurement data collected,
  - Perform first level analysis of the collected data, and,

<sup>202</sup> 

<sup>&</sup>lt;sup>1</sup> The way this actual measurement is performed is not a subject of standardisation within FIPA.

- 203 Send the results of the analysis to CA, if requested to do so.
- 205 A CA may:
- 207 Manage (establish, close, suspend, activate, etc.) an MTC<sup>2</sup>.

In some cases there is a need for MAs and CAs in heterogeneous APs to communicate with each other; therefore, interaction protocols and ontologies to achieve this are specified in this document.

211

204

206

208

#### 212 **2.3 Negotiation of Message Transport Requirements**

There are several mechanisms that can determine the MTP, message representation and content language to use between communicating entities:

- 215216 Communicating entities know a peer entity's preferences beforehand and use them.
- The activating entity tries to use a method and if the peer entity is not capable of using the suggested method, then the activating entity may try another one (and so on).
- 221 The communicating entities negotiate about a method to be used.
- 222

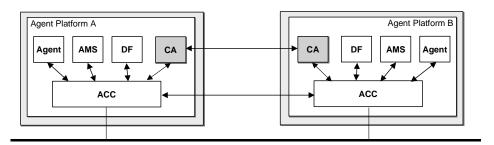
217

220

#### 223 **2.3.1 Negotiation About Message Transport Protocols**

Previous FIPA specifications have implicitly assumed that the MTC is operational all the time (meaning that the MTC has been established before the agent message exchange and that it is reliable). However, this is not always the case within a nomadic environment.

- A CA can activate the selection of an MTP or an agent can propose an MTP to a CA and it is the responsibility of the CA to either accept or reject the proposal based on whether it is possible to use the proposed MTP. CAs negotiate with peer CAs to use proposed MTPs which is illustrated in *Figure 2*.
- 231



232 233

233 235

Figure 2: Control Agents Negotiating About a Message Transport Protocol

CAs use the FIPA-Propose interaction protocol [FIPA00036] and the use action to negotiate about an MTP. An example negotiation is given in section *5.2, Negotiating Message Transport Protocols*.

238

#### 239 2.3.2 Negotiation About Message Representation

In the environment of nomadic applications, it may be necessary to switch from one ACL representation to another; for example, when a mobile host roams from a wireline network to a wireless network. Application agents may use the FIPA-Propose interaction protocol and the use action to negotiate about the representation of ACL. Examples of this negotiation are given in section *5.3, Negotiating Message Representation*.

<sup>&</sup>lt;sup>2</sup> The way that management actions are executed is not a subject of standardisation within FIPA.

# 244 **3 Nomadic Application Support Ontology**

245 The FIPA-Nomadic-Application ontology is a combination of FIPA-MTS-QoS, FIPA-Communication 246 Management, and FIPA-Message-Representation ontologies.

#### 247 3.1 Object Descriptions

- This section describes a set of frames, that represent the classes of objects in the domain of discourse within the framework of the FIPA-Nomadic-Application ontology.
- 251 The following terms are used to describe the objects of the domain:
- 253 Frame. This is the mandatory name of this entity, that must be used to represent each instance of this class.
- Ontology. This is the name of the ontology, whose domain of discourse includes the parameters described in the table.
   257
- 258 **Parameter**. This is the mandatory name of a parameter of this frame.
- 260 **Description**. This is a natural language description of the semantics of each parameter.
- 262 **Presence**. This indicates whether each parameter is mandatory or optional.
- **Type**. This is the type of the values of the parameter: Integer, Word, String, URL, Term, Set or Sequence.
  - **Reserved Values**. This is a list of FIPA-defined constants that can assume values for this parameter.

#### 266 267

252

254

259

261

263

265

#### 268 3.1.1 Quality of Service Description

- 269 This type of object represents the quality of service of the transport protocol or communication channel.
- 270

Frame Ontology	qos FIPA-MTS-QoS			
Parameter	Description	<b>Presence</b> <sup>3</sup>	Туре	Reserved Values
line-rate	The bandwidth in one direction over the link.	Optional	rate-value	
throughput	The number of user data bits successfully transferred in one direction across the link <sup>4</sup> . Successful transfer means that no user data bits are lost, added or inverted in transfer.	Optional	rate-value	
throughput- std-dev	The current standard deviation of the throughput within a time unit.	Optional	rate-value	
rtt	The round trip time which is the time required for a data segment to be transmitted to a peer entity and a corresponding acknowledgement sent back to the originating entity.	Optional	time-value	
rtt-std-dev	The standard deviation of the round-trip time within a time unit.	Optional	time-value	

<sup>&</sup>lt;sup>3</sup> While all of the parameters for this object are optional, a valid gos object will contain at least one parameter. <sup>4</sup> See [ITUX135].

delay	The (nominal) time required for a data segment to be transmitted to a peer entity.	Optional	time-value	
delay-std-dev	The standard deviation of the delay time within a time unit.	Optional	time-value	
mean-up-time	The expected uptime of an established link.	Optional	time-value	
omission-rate	The probability that a data segment is not transmitted correctly over a link.	Optional	probability- value	
ber	The ratio of the number of bit errors to the total number of bits transmitted in a given time interval <sup>5</sup> .	Optional	probability- value	
frame-error- rate	The probability that a data segment is not transmitted correctly over a link.	Optional	probability- value	
conn-setup- delay	The (sampled) delay to establish a connection between communicating entities.	Optional	time-value	
conn-setup- failure-prob	The ratio of total call attempts that result in call setup failure to the total call attempts in a population of interest.	Optional	probability- value	
status	The connectivity status of the link. Connected means that there (at least) logical connection between communicating entities. Disconnected means that there is no connection between communicating entities, and the communicating entities are not establishing a connection at the moment. Connecting means that there is no connection between communicating entities, but they are currently establishing a connection between them.	Optional	Word	Connected Disconnected Connecting

#### 271 3.1.2 Rate Value

272 This type of object represents a data transfer value.

273

Frame Ontology	rate-value FIPA-MTS-QoS			
Parameter	Description	Presence	Туре	Reserved Values
direction	The direction in which this value is measured. Inbound means the data transmission where the actor receives the data, and outbound means the data transmission where the actor transmits the data.	Mandatory	Word	Inbound Outbound

<sup>₅</sup> See [ITUE800].

unit	The unit in which the value is represented. Bits/s means bits per seconds. Kbits/s means kilobits per seconds. One kilobit is 2^10 bits. Mbits/s means megabits per second. One megabit is 2^20 bits. Gbits/s means gigabits per second. One gigabit is 2^30 bits.	Mandatory	Word	GBits/s MBits/s KBits/s Bits/s
value	The rate value.	Mandatory	Number	

#### 275 3.1.3 Time Value

276 This type of object represents a time value.

277

Frame Ontology	time-value FIPA-MTS-QoS			
Parameter	Description	Presence	Туре	Reserved Values
direction	The direction in which this value is measured. Inbound means the data transmission where the actor receives the data, and outbound means the data transmission where the actor transmits the data.	Optional <sup>6</sup>	Word	Inbound Outbound
unit	The unit in which the value is represented. h means hours, m means minutes, s means seconds, and ms means milliseconds.	Mandatory	Word	h m s ms
value	The time value.	Mandatory	Number	

#### 278

#### 279 3.1.4 Probability Value

280 This type of object represents a probability value.

#### 281

Frame Ontology	probability-value FIPA-MTS-QoS			
Parameter	Description	Presence	Туре	Reserved Values
direction	The direction in which this value is measured. Inbound means the data transmission where the actor receives the data, and outbound means the data transmission where the actor transmits the data.	Optional	Word	Inbound Outbound
value	The probability value which obeys the following axiom: 0 • value • 1	Mandatory	Number	

<sup>&</sup>lt;sup>6</sup> This parameter is mandatory for those QoS values that have a different value depending upon the direction.

#### 283 3.1.5 Change Constraint

- 284 This type of object represents constraints that limit quality of service notifications.
- 285

Frame Ontology	change-constraint FIPA-MTS-QoS			
Parameter	Description	Presence	Туре	Reserved Values
value	The description of the	Mandatory	Expression	
	constraints.			

286

#### 287 3.1.6 Time Constraint

288 This type of object represents constraints that limit quality of service notifications.

289

Frame Ontology	time-constraint FIPA-MTS-QoS			
Parameter	Description	Presence	Туре	Reserved Values
type	The type of the constraint. If the type Every is used, then the expression becomes true after value and thereafter at intervals of value. If the type After is used, then the expression becomes true only after value.	Mandatory	Word	Every After
value	The time value.	Mandatory	time-value	

290

#### 291 3.1.7 Communication Channel Description

292 This type of object represents a communication channel.

293

Frame Ontology	comm-channel FIPA-Communication-Management			
Parameter	Description	<b>Presence</b> <sup>7</sup>	Туре	<b>Reserved Values</b>
name	The logical name of the communication channel.	Optional	Word	
target-addr	The target transport address of the communication channel. This may also be the address of a gateway ACC.	Optional	URL	
options	A list of optional parameters for the communication channel.	Optional	Set of property (see [FIPA00023])	

<sup>&</sup>lt;sup>7</sup> Either the :name parameter or the :target-addr parameter must be present in this object.

#### 295 3.1.8 Transport Protocol Description

- 296 This type of object represents a transport protocol.
- 297

Frame Ontology	transport-protocol FIPA-Communication-Management			
Parameter	Description	Presence	Туре	Reserved Values
Name	The logical name of the transport protocol.	Mandatory	Word	
gw-addr	The transport address of the gateway ACC.	Optional	URL	
dest-addr	The transport address of the ultimate destination. If this address is present, but gw-addr is not, then the Control Agent may select the most appropriate gateway transport address to use.	Optional	URL	
options	A list of optional parameters for the transport protocol.	Optional	Set of property	

298

#### 299 3.1.9 Transport Protocol Selection

300 This type of object represents a selection of transport protocol.

301

Frame Ontology	transports FIPA-Communication-Management			
Parameter	Description	Presence	Туре	<b>Reserved Values</b>
send	A list of transport protocols supported for sending messages.	Mandatory	Sequence of transport- protocol	
recv	A list of transport protocols supported for receiving messages.	Mandatory	Sequence of transport- protocol	

302

#### 303 3.1.10 Message Representation Description

304 This type of object represents an ACL message representation.

305

Frame Ontology	msg-representation FIPA-Message-Representation			
Parameter	Description	Presence	Туре	Reserved Values
Name	The name of the message representation.	Mandatory	Word	See [FIPA00068]
Options	A list of parameters for the message representation.	Optional	Set of property	

#### 307 3.1.11 Message Representation Selection

- 308 This type of object represents a selection of message representations.
- 309

Frame Ontology	msg-rep-selection FIPA-Message-Representation			
Parameter	Description	Presence	Туре	Reserved Values
send	A list of message representations supported for sending messages.	Mandatory	Sequence of msg- representation	
recv	A list of message representations supported for receiving messages.	Mandatory	Sequence of msg- representation	

310

311

#### 312 **3.2 Function and Predicate Descriptions**

The following tables define usage and semantics of the functions and the predicates that are part of the FIPA-Nomadic-Application ontology.

- 316 The following terms are used to describe the functions of the FIPA-Nomadic-Application domain:
  - **Function**. This is the symbol that identifies the function in the ontology.
- 320 **Predicate**. This is the symbol that identifies the predicate in the ontology.
- 322 **Ontology**. This is the name of the ontology, whose domain of discourse includes the function or the predicate 323 described in the table.
- 325 **Supported by**. This is the type of agent that supports this function or predicate.
- 327 **Description**. This is a natural language description of the semantics of the function or the predicate.
- **Domain**. This indicates the domain over which the function predicate is defined. The arguments passed to the function or predicate must belong to the set identified by the domain.
- Range. This indicates the range to which the function maps the symbols of the domain. The result of the function isa symbol belonging to the set identified by the range.
- Arity. This indicates the number of arguments that a function or a predicate takes. If a function or a predicate can take an arbitrary number of arguments, then its arity is undefined.
- 337

334

315

317 318

319

321

324

326

328

#### 338 3.2.1 Request Monitoring Information

	0	
Predicate	qos-information	
Ontology	FIPA-Nomadic-Application	
Supported by	MA	
Description	protocol (see [FIPA00027]). The a protocol to request quality of service The predicate is true, when the va for given communication channel of transport protocol is what stated in	lues of the QoS parameters defined in the QoS object are true or transport protocol (i.e., the QoS of communication channel or the QoS object). Otherwise the predicate is false.
Domain	comm-channel /8 transport-pr	rotocol, <sup>°</sup> qos
Arity	2	

<sup>&</sup>lt;sup>8</sup> Where '/' is "exclusive or".

<sup>&</sup>lt;sup>9</sup> Where ',' is "and".

#### 340 3.2.2 Subscribe to Changes

Predicate	qos-notification
Ontology	FIPA-Nomadic-Application
Supported by	MA
Description	An agent subscribes to notifications about changes to the quality of service from an MA using the FIPA-Subscribe interaction protocol (see [FIPA00035]). The predicate is true, when the values of the QoS parameters defined in the QoS object are true for given communication channel or transport protocol, and the given constraints are met Otherwise the predicate is false.
Domain	comm-channel, qos, change-constraints / time-constraints
Arity	3

341

### 342 3.2.3 Open Communication Channel

Function	open-comm-channel
Ontology	FIPA-Nomadic-Application
Supported by	CA
Description	An agent can request that a CA open a communication channel. The communication channel description should contain enough information for a CA to be able to choose the right communication channel, that is, either the :name parameter or the :target-addr parameter must be present. The agent may also supply additional communication channel information by using the :options parameter.
Domain	comm-channel
Range	The execution of this function results in a change of the state, but it has no explicit result. Therefore there is no range set.
Arity	1

343

#### 344 3.2.4 Close Communication Channel

Function	close-comm-channel	
Ontology	FIPA-Nomadic-Application	
Supported by	CA	
Description	An agent can request that a CA close a communication channel. The communication channel description should contain enough information for a CA to be able to choose the righ communication channel, that is, either the :name parameter or the :target-addr parameter must be present.	
Domain	comm-channel	
Range	The execution of this function results in a change of the state, but it has no explicit result. Therefore there is no range set.	
Arity	1	

#### 346 3.2.5 Activate a Message Transport Protocol

Function	activate	
Ontology	FIPA-Nomadic-Application	
Supported by	CA	
Description	protocol description should contain transport protocol. Additionally, the	activate a Message Transport Protocol (MTP). The transport in enough information to allow the CA to identify the correct e agent may supply address information to where the transport ned. It is possible to give the address of the gateway and/or the
Domain	Sequence of transport-protoc	col
Range	transport-protocol	
Arity	1	

347

#### 348 3.2.6 Deactivate a Message Transport Protocol

Function	deactivate	
Ontology	FIPA-Nomadic-Application	
Supported by	CA	
Description	An agent can request that a CA deacti	vate an MTP.
Domain	transport-protocol	
Range	The execution of this function results in a change of the state, but it has no explicit result. Therefore there is no range set.	
Arity	1	

349

#### 350 **3.2.7 Select a Message Transport Protocol**

Function	use	
Ontology	FIPA-Nomadic-Application	
Supported by	CA	
Description	Channels (ACCs) using the FII requesting CA shall provide enou direction of communication (either The list of MTPs is an ordered list w	to select an MTP for use between Agent Communication PA-Propose interaction protocol (see [FIPA00036]). The gh information to establish a working MTP connection. The send, receive or both) and the list of MTPs must be present. where the highest priority is the first item and the lowest priority receiving CA shall select at most one MTP for the proposed send, receive or both)
Domain	transports	
Range	transports	
Arity	1	

351

## 352 3.3 Exceptions

The exceptions for the FIPA-Nomadic-Application ontology follow the same form and rules as specified in [FIPA00023].

355

#### 356 3.3.1 Not Understood Exception Propositions

357The same set of "Not Understood Exception Propositions" as in the FIPA-Agent-Management ontology is used in the358FIPA-Nomadic-Application ontology (see [FIPA00023]).

#### 360 3.3.2 Refusal Exception Propositions

361 The same set of "Refusal Exception Propositions" as defined in the FIPA-Agent-Management ontology is used in

362 FIPA-Nomadic-Application ontology (see [FIPA00023]). In addition, the FIPA-Nomadic-Application ontology 363 defines the propositions given below.

364

Communicative Act Ontology	Refuse FIPA-Nomadic- Application	
Predicate symbol	Arguments	Description
already-open	String	The specified communication channel is already open; the string identifies the communication channel.
not-open	String	The specified communication channel is not open; the string identifies the communication channel.
already-activated	String	The specified transport protocol is already activated; the string identifies the transport protocol.
not-active	String	The specified transport protocol is not active; the string identifies the transport protocol.
unrecognised-comm-channel	String	The specified communication channel is not recognised; the string identifies the communication channel.
unsupported-protocol	String	The specified transport protocol is not supported; the string identifies the transport protocol.

365

#### 366 3.3.3 Failure Exception Propositions

Communicative Act Ontology	failure FIPA-Agent-Management	
Predicate symbol	Arguments	Description
internal-error	String	See [FIPA00023].
open-failed	String	The opening of a communication channel failed; the string identifies the failure reason.
transient-failed	String	The opening/closing of a communication channel or the activation/deactivation of a transport protocol failed; the string identifies the failure reason.
close-failed	String	The closing of a communication channel failed; the string identifies the failure reason.
activation-failed	String	The activation of a transport protocol failed; the string identifies the failure reason.
deactivation-failed	String	The deactivation of a transport protocol failed; the string identifies the failure reason.

376

378

381

384

386

389

392

# 367 4 Registration of the Control Agent and Monitor Agent with the DF

- In order for a Control Agent and Monitor Agent to advertise its willingness to provide its services to an agent domain, it
   must register with a DF (as described in [FIPA00023].
- As part of this registration process following of constant values are introduced that universally identify the services the agent provides:
- The name slot in service-description frame of a Control Agent must be declared as a constant fipa-mtscontrol.
- 377 The type slot in service-description frame of a Control Agent must be declared as a constant fipa-ca.
- The ontology slot in service-description frame of a Control Agent should be declared as a constant fipa nomadic-application or a constant fipa-communication-management.
- 382 The type slot in service-description frame of a Monitor Agent must be declared as a constant fipa-mts-383 monitor.
- 385 The type slot in service-description frame of a Monitor Agent must be declared as a constant fipa-ma.
- The ontology slot in service-description frame of a Monitor Agent should be declared as a constant fipa nomadic-application.
- Below is given an example content of a agent df-agent-description frame which provides both MA and CA functionality:

```
393
      (df-agent-description
394
        :name
395
          (agent-identifier
396
            :name monitor&control agent@iiop://foo.com/acc
397
            :addresses (sequence iiop://foo.com/acc))
398
        :protocols (set fipa-request fipa-propose fipa-subscribe)
399
        :ontology (set fipa-nomadic-application)
400
        :language (set fipa-sl0)
401
        :services (set
402
          (service-description
403
            :name fipa-mts-control
404
            :type fipa-ca
405
            :ontology fipa-nomadic-application)
406
          (service-description
407
                  :name fipa-mts-monitor
408
                  :type fipa-ma
409
                  :ontology fipa-nomadic-application))
410
              :ownership (set Sonera)))))
411
```

#### 411 **5 Scenarios**

#### 412 5.1 Registration with a DF

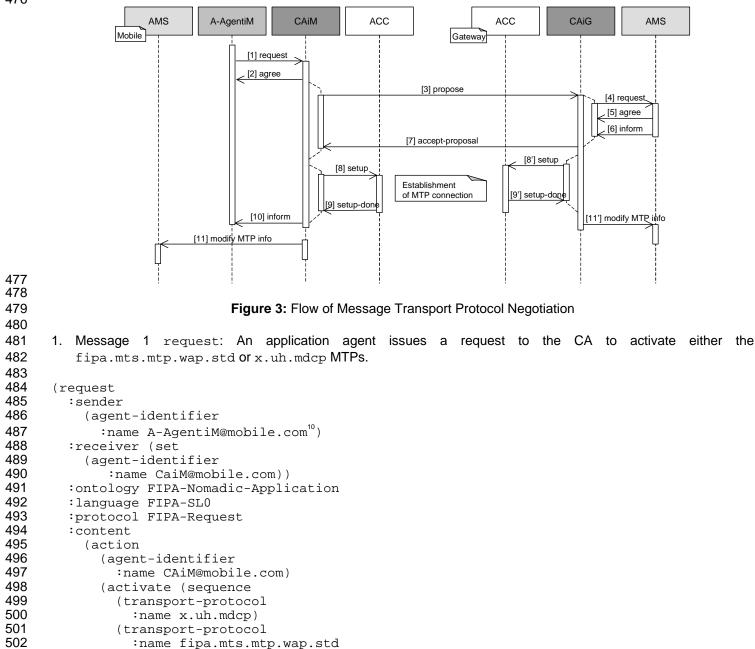
```
413
      1. A CA registers with a DF (see [FIPA00023]):
414
415
      (request
416
        :sender
417
          (agent-identifier
418
            :name ca@foo.com
419
            :addresses (sequence http://foo.com/acc))
420
        :receiver (set
421
          (agent-identifier
422
            :name df@foo.com
423
            :addresses (sequence http://foo.com/acc)))
424
        :language FIPA-SL0
425
        :protocol FIPA-Request
426
        :ontology FIPA-Agent-Management
        :content
427
428
          (action
429
            (agent-identifier
430
              :name df@foo.com
431
              :addresses (sequence http://foo.com/acc))
432
            (register
433
              (df-agent-description
434
                :name
435
                   (agent-identifier
436
                     :name ca@foo.com
437
                     :addresses (sequence http://foo.com/acc))
438
                :services (set
439
                   (service-description
440
                     :name fipa-mts-control
441
                     :type fipa-ca
442
                     :ontology (set FIPA-Nomadic-Application))))))))
443
444
      2. A MA registers with a DF:
445
      (request
446
        :sender
447
          (agent-identifier
448
            :name ma@foo.com
449
            :addresses (sequence http://foo.com/acc))
450
        :receiver (set
451
          (agent-identifier
452
            :name df@foo.com
453
            :addresses (sequence http://foo.com/acc)))
454
        :language FIPA-SL0
455
        :protocol FIPA-Request
456
        :ontology FIPA-Agent-Management
457
        :content
458
          (action
459
            (agent-identifier
460
              :name df@foo.com
461
               :addresses (sequence http://foo.com/acc))
462
            (register
463
              (df-agent-description
464
                 :name
465
                   (agent-identifier
466
                     :name ma@foo.com
467
                     :addresses (sequence http://foo.com/acc))
468
                :services (set
469
                   (service-description
```

504 505

470:name fipa-mts-monitor471:type fipa-ma472:ontology (set FIPA-Nomadic-Application)))))))

#### 473 5.2 Negotiating Message Transport Protocols

This example shows a scenario, where an application agent requests the use of either the WAP MTP [FIPA00076] or a proprietary MTP (for example, x.uh.mdcp). The message flow of a successful negotiation is illustrated in *Figure 3*.



:dest-addr wap://gateway.com:1234/acc))))

<sup>&</sup>lt;sup>10</sup> In all of the examples in this specification, the suffix of iM in an agent's name represents a mobile host, that is, an agent that is located on a mobile AP. Similarly, the suffix iG represents a gateway host and the suffix iF represents a fixed network host.

 Message 2 agree: The CA agrees to activate an MTP. The decision to agree or disagree to activate an MTP might be based on the internal state of the CA (that is, the CA knows whether a requested MTP can be activated or not) or the CA might ask for an AP description from an AMS.

```
508
509
      (agree
510
        :sender
          (agent-identifier
511
512
            :name CAiM@mobile.com)
513
        :receiver (set
          (agent-identifier
514
            :name A-AgentiM@mobile.com))
515
        :ontology FIPA-Nomadic-Application
516
517
        :language FIPA-SL0
518
        :protocol FIPA-Request
519
        :content
520
          ((action
521
            (agent-identifier
              :name CAiM@mobile.com))
522
523
           (activate (sequence
524
             (transport-protocol
525
                :name x.uh.mdcp)
526
              (transport-protocol
527
                :name fipa.mts.mtp.wap.std
528
                :dest-addr wap://gateway.com:1234/acc))))
529
          true))
530
```

Message 3 propose: The CA in the mobile host proposes to its peer CA in the gateway host that either the
 fipa.mts.mtp.wap.std or x.uh.mdcp MTPs should be used in communication between the APs.

```
<?xml version="1.0"?><sup>11</sup>
534
535
536
      <envelope>
537
538
        <params index="1">
539
540
          <to>
541
             <agent-identifier>
542
               <name>CAiG@gateway.com</name>
543
             </agent-identifier>
544
          </to>
545
          <from>
546
             <agent-identifier>
547
               <name>CAiM@mobile.com</name>
548
             </agent-identifier>
549
          </from>
550
551
          <acl-representation>fipa.acl.rep.string.std</acl-representation>
552
553
           <date>20000606T100900000</date>
554
555
        </params>
556
557
      </envelope>
558
559
      (propose
560
        :sender
561
           (agent-identifier
562
             :name CAiM@mobile.com)
563
        :receiver (set
564
           (agent-identifier
```

<sup>&</sup>lt;sup>11</sup> In most of the examples, the envelope part has been omitted for clarity.

```
565
             :name CAiG@gateway.com))
566
        :ontology FIPA-Nomadic-Application
567
        :language FIPA-SL0
568
        :protocol FIPA-Propose
569
        :content
570
           ((action
571
             (agent-identifier
572
               :name CAiM@mobile.com)
573
             (use
574
               (transports
575
                 :send (sequence
576
                   (transport-protocol
577
                      :name x.uh.mdcp)
578
                   (transport-protocol
579
                     :name fipa.mts.mtp.wap.std))
580
                 :recv (sequence
581
                   (transport-protocol
582
                      :name x.uh.mdcp)
583
                   (transport-protocol
584
                      :name fipa.mts.mtp.wap.std)))))
585
          true))
586
587
      4. Message 4 request, message 5 agree and message 6 inform: The CA in the gateway host requests the AP
         description from the local AMS (see [FIPA00023]) to determine whether the x.uh.mdcp or
588
         fipa.mts.mtp.wap.std MTPs are supported. The AMS informs the CA that both MTPs are supported and the
589
         CA decides to use fipa.mts.mtp.wap.std MTP based on the current quality of service requirements of the
590
591
         MTC.
592
593
      (request
594
        :sender
595
          (agent-identifier
596
            :name CAiG@gateway.com)
597
        :receiver (set
598
           (agent-identifier
599
             :name ams@gateway.com))
        :ontology FIPA-Agent-Management
600
        :language FIPA-SL0
601
602
        :protocol FIPA-Request
603
        :content
604
          (action
605
             (agent-identifier
606
               :name ams@gateway.com)
607
          get-description))
608
609
      (agree
610
        :sender
611
          (agent-identifier
612
            :name ams@gateway.com)
613
        :receiver (set
           (agent-identifier
614
             :name CAiG@gateway.com))
615
616
        :ontology FIPA-Agent-Management
617
        :language FIPA-SL0
618
        :protocol FIPA-Request
619
        :content
620
          ((action
621
             (agent-identifier
622
               :name ams@gateway.com)
623
            get-description)
624
          true))
625
626
      (inform
627
        :sender
```

690

:send (sequence

(transport-protocol

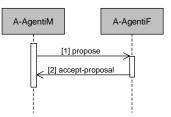
```
628
          (agent-identifier
629
            :name ams@gateway.com
630
            :addresses (sequence http://gateway.com/acc))
631
        :receiver (set
632
          (agent-identifier
633
            :name CAiG@gateway.com
634
            :addresses (sequence http://gateway.com/acc)))
635
        :ontology FIPA-Agent-Management
636
        :language FIPA-SL0
637
        :protocol FIPA-Request
638
        :content
639
          (ap-description
640
            :name sonera-platform
641
            :transport-profile
642
               (ap-transport-description
643
                 :available-mtps
644
                   (set
645
                     (mtp-description
646
                         :profile fipa.profile.mts.alpha
647
                         :mtp-name fipa.mts.mtp.iiop.std
648
                         :addresses (sequence iiop://gateway.com/acc))
649
                     (mtp-description
650
                         :profile fipa.profile.mts.beta
651
                         :mtp-name fipa.mts.mtp.wap.std
652
                         :addresses (sequence wap://gateway.com:1234/acc))
653
                     (mtp-description
654
                         :profile x.uh.profile
655
                         :mtp-name x.uh.mdcp
656
                         :addresses (set mdcp://gateway.com/acc)))))
657
658
      5. Message 7 accept-proposal: The CA in the gateway host accepts the proposal to use the
         fipa.mts.mtp.wap.std MTP and sends the response to the CA in the mobile host informing it about the
659
660
         preferred MTP.
661
662
      (accept-proposal
663
        :sender
664
          (agent-identifier
665
            :name CAiG@gateway.com)
666
        :receiver (set
667
          (agent-identifier
668
            :name CAiM@mobile.com))
669
        :ontology FIPA-Nomadic-Application
670
        :language FIPA-SL0
671
        :protocol FIPA-Propose
672
        :content
673
          (action
674
            (agent-identifier
675
               :name CAiM@mobile.com)
676
             (use
677
               (transports
678
                 :send (sequence
679
                   (transport-protocol
680
                     :name x.uh.mdcp)
681
                   (transport-protocol
682
                     :name fipa.mts.mtp.wap.std))
683
                 :recv (sequence
684
                   (transport-protocol
685
                     :name x.uh.mdcp)
686
                   (transport-protocol
687
                     :name fipa.mts.mtp.wap.std)))))
688
          (transports
```

```
691
                  :name fipa.mts.mtp.wap.std))
692
             :recv (sequence
693
               (transport-protocol
694
                  :name fipa.mts.mtp.wap.std))))
695
696
      6. Messages 8 and 8' setup: The CAs request their respective ACCs to setup the fipa.mts.mtp.wap.std MTP.
697
         This is an implementation issue.
698
699
      7. Message 9 and 9' setup-done: The ACCs inform their respective CAs that the fipa.mts.mtp.wap.std MTP
700
         has been established between the mobile host and the gateway host.
701
702
      8. Message 10 inform: The CA informs the application agent that the MTC is established.
703
704
      (inform
705
         :sender
706
           (agent-identifier
707
             :name CAiM@mobile.com)
708
         :receiver (set
709
           (agent-identifier
710
             :name A-AgentiM@mobile.com))
711
         :ontology FIPA-Nomadic-Application
712
        :language FIPA-SL0
713
         :protocol FIPA-Request
714
         :content
715
           (result
716
             (action
717
               (agent-identifier
718
                  :name CaiM@mobile.com)
719
             (activate (sequence
720
               (transport-protocol
721
                  :name x.uh.mdcp)
722
                (transport-protocol
723
                  :name fipa.mts.mtp.wap.std
724
                  :dest-addr wap://gateway.com:1234/acc))))
725
           (transport-protocol
726
             :name fipa.mts.mtp.wap.std))
727
      9. Message 11 and 11' set-description: CAiM (/CAiG) modifies the AP description to show that the
728
729
          fipa.mts.mtp.wap.std is now active.
730
```

731 5.3 Negotiating Message Representations

This example shows a scenario where an application agent in a mobile host proposes to its peer application agent in a fixed host the use of the fipa.acl.rep.bitefficient.std representation of ACL [FIPA00069] for their communication. The message flow is illustrated in *Figure 4*.

735



736 737

- 738
- 739

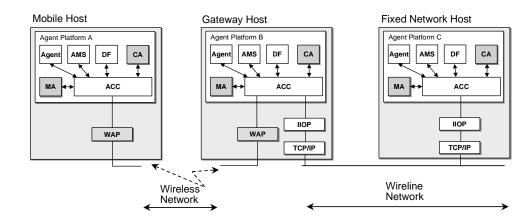
Figure 4: Flow of Message Representation Negotiation

Message 1 propose: The agent in the mobile host proposes the use of the fipa.acl.rep.bitefficient.std
 representation of ACL.

```
743
      (propose
744
        :sender
745
          (agent-identifier
746
            :name A-AgentiM@mobile.com)
747
        :receiver (set
748
          (agent-identifier
749
             :name A-AgentiF@fixed.com))
750
        :ontology FIPA-Message-Representation
751
        :language FIPA-SL0
752
        :protocol FIPA-Propose
753
        :content
754
          ((action
755
             (agent-identifier
               :name A-AgentiM@mobile.com)
756
757
             (use
758
               (msq-rep-selection
759
                 :send (sequence
760
                   (msg-representation
761
                     :name fipa.acl.rep.bitefficient.std))
762
                 :recv (sequence
763
                   (msg-representation
764
                     :name fipa.acl.rep.bitefficient.std)))))
765
            true))
766
767
      2. Message 2 accept-proposal: The agent in the fixed host accepts the proposal.
768
769
      (accept-proposal
770
        :sender
771
          (agent-identifier
772
             :name A-AgentiF@fixed.com)
773
        :receiver (set
774
          (agent-identifier
775
             :name A-AgentiM@mobile.com))
776
        :ontology FIPA-Message-Representation
777
        :language FIPA-SL0
778
        :protocol FIPA-Propose
779
        :content
780
          (action
781
             (agent-identifier
782
               :name A-AgentiM@mobile.com)
783
             (use
784
               (msg-rep-selection
785
                 :send (sequence
786
                   (msg-representation
787
                     :name fipa.acl.rep.bitefficient.std))
788
                 :recv (sequence
                   (msg-representation
789
790
                     :name fipa.acl.rep.bitefficient.std))))
791
             (msg-rep-selection
792
               :send (sequence
793
                 (msg-representation
794
                   :name fipa.acl.rep.bitefficient.std))
795
               :recv (sequenc
796
                 (msg-representation
797
                   :name fipa.acl.rep.bitefficient.std))))
798
```

#### 799 5.4 Message Exchange Over a WAP Message Transport Protocol

Figure 5 refers to reference architecture for message exchange in context of nomadic applications. Messages between the mobile host and gateway host are delivered mainly using the fipa.mts.mtp.wap.std MTP and messages between gateway host and other APs in the fixed network are delivered using the fipa.mts.mtp.iiop.std MTP (see [FIPA00075]).



804

Figure 5: Gateway-Based Nomadic Application Architecture

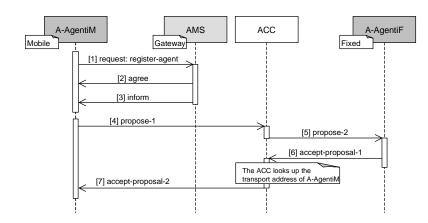
- 806
- 807 808

#### 809 **5.4.1** Message Exchange Activation by an Agent in a Mobile Host

This example shows the scenario where an agent in a mobile host has a WAP address and an agent in fixed host has an IIOP address. In this example, there are three specific APs involved: one running in a mobile host, one running in a

an IIOP address. In this example, there are three specific APs involved; one running in a mobile host, one running in a gateway host and the last one running in a host situated in a fixed network which represents the rest of the network. An

- 813 example of the flow of a message exchange is illustrated in *Figure 6*.
- 814



815 816 817

- Figure 6: Mobile Originated Message Exchange Over Gateway Host
- Message 1 request, message 2 agree and message 3 inform: In order to be reachable from an AP operating in a fixed network environment, an agent in the mobile host must register with the AP running in the gateway host.
   Subsequently, the ACC in the gateway host AP can forward messages intended for the agent operating in the mobile host to the ACC.

```
823
824
      (request
825
        :sender
826
          (agent-identifier
827
             :name A-AgentiM@mobile.com)
828
        :receiver (set
829
          (agent-identifier
830
             :name ams@gateway.com))
831
        :language FIPA-SL0
832
        :protocol FIPA-Request
        :ontology FIPA-Agent-Management
833
834
        :content
835
          (action
836
             (agent-identifier
837
               :name ams@gateway.com)
```

```
838
             (register
839
               (ams-agent-description
840
                  :name
841
                    (agent-identifier
842
                      :name A-AgentiM@mobile.com
843
                      :addresses (sequence wap://mobile.com:1234/acc))
844
                  :state active))))
845
846
      The AMS informs A-AgentiM that registration was completed successfully and after registration, A-AgentiM can be
847
      reached via the gateway host using, for example, the following to envelope parameter:
848
849
      <to>
850
         <agent-identifier>
851
           <name>A-AgentiM@mobile.com</name>
852
           <addresses>
853
             <url>iiop://gateway.com/acc</url>
854
           </addresses>
855
         </agent-identifier>
856
      </to>
857
858
      If the gateway host is not operational, then the direct WAP address (wap://mobile.com:1234/acc) could be used.
859
860
      2. Message 4 propose 1: A-AgentiM sends a propose message to A-AgentiF. In the from envelope parameter,
861
         A-AgentiM informs A-AgentiF that its primary return address is its address in the gateway host.
862
863
      <?xml version="1.0"?>
864
      <envelope>
865
         <params index="1">
866
           <to>
             <agent-identifier>
867
868
               <name>A-AgentiF@fixed.com</name>
869
               <addresses>
870
                 <url>iiop://fixed.com/acc</name>
871
               </addresses>
872
             </agent-identifier>
873
           </to>
874
           <from>
875
             <agent-identifier>
876
               <name>A-AgentiM@mobile.com</name>
877
               <addresses>
878
                 <url>iiop://gateway.com/acc</url>
879
                  <url>wap://mobile.com:1234/acc>/url>
880
               </addresses>
881
             </aqent-identifier>
882
           </from>
883
           <acl-representation>fipa.acl.rep.string.std</acl-representation>
884
           <date>20000606T100900000</date>
885
         </params>
886
      </envelope>
887
888
      (propose
889
         :sender
890
           (agent-identifier
891
             :name A-AgentiM@mobile.com)
         :receiver (set
892
893
           (agent-identifier
894
             :name A-AgentiF@fixed.com))
895
         :language FIPA-SL0
896
         :content
897
           (action
898
             (agent-identifier
899
               :name A-AgentiM@mobile.com)
900
             (compress-data (> object-size 1kb)))
```

902 The ACC in the mobile host forwards the message to the ACC in the gateway host using fipa.mts.mtp.wap.std 903 MTP<sup>12</sup>.

- 3. Message 5 propose 2: The ACC in the gateway host forwards the message to A-AgentiF using
   fipa.mts.mtp.iiop.std MTP. The ACC may change the encoding of the message.
- 908 4. Message 6 accept-proposal 1: A-AgentiF accepts A-AgentiM's proposal by sending an accept 909 proposal message to A-AgentiM using its gateway host address.

```
910
911
      (accept-proposal
912
        :sender
913
          (agent-identifier
914
             :name A-AgentiF@fixed.com)
915
        :receiver (set
916
          (agent-identifier
917
             :name A-AgentiM@mobile.com))
918
        :language FIPA-SL0
919
        :content
920
          ((action
921
             (agent-identifier
922
               :name A-AgentiM@mobile.com)
923
             (compress-data (> object-size 1kb)))
924
          true))
925
```

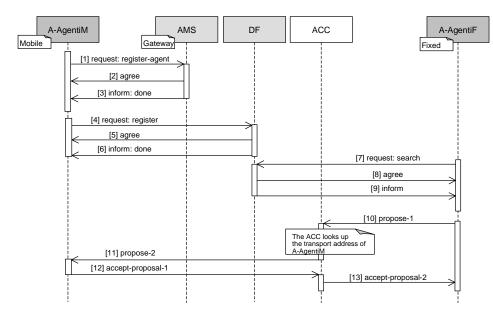
- Message 7 accept-proposal 2: The ACC in the gateway host forwards the message to the ACC in the mobile host using the fipa.mts.mtp.wap.std MTP. The ACC may change the encoding of the message.
- 929 5.4.2 Message Exchange Termination to an Agent in a Mobile Host

930 This example shows the scenario where an agent in a fixed host activates a conversation. The message flow is 931 illustrated in *Figure 7*.

932

901

907



933 934

935 936 Figure 7: Mobile Terminated Message Exchange Over Gateway Hosts

Message 1 request, message 2 agree and message 3 inform: See Section 5.4.1, Message Exchange
 Activation by an Agent in a Mobile Host.

<sup>&</sup>lt;sup>12</sup> The actual way in which the is achieved in not a subject of standardisation within FIPA.

942 943

(request

Message 4 request: A-AgentiM needs to register its services with the DF in the gateway host in order to be able to publicise its services even when the mobile host itself is disconnected from the fixed network.

```
944
         :sender
945
           (agent-identifier
946
             :name A-AgentiM@mobile.com)
947
         :receiver (set
948
           (agent-identifier
949
             :name df@gateway.com))
950
         :ontology FIPA-Agent-Management
         :language FIPA-SL0
951
952
         :protocol FIPA-Request
953
         :content
954
           (action
             (agent-identifier
955
956
                :name df@qateway.com)
957
             (register
958
                (df-agent-description
959
                  :name
960
                    (agent-identifier
961
                      :name A-AgentiM@mobile.com
962
                      :addresses (sequence iiop://gateway.com/acc wap://mobile.com:1234/acc))
963
                  :services (set
964
                    (service-description
965
                      :name Field-Warrior
 966
                      :type field-information
967
                      :ontology (set field-service)
968
                      :properties (set
969
                        (property
970
                          :name availability
971
                          :value 24h))))
972
                  :language (set FIPA-SL0))))
973
974
       3. Message 5 agree and message 6 inform: The DF in the gateway host AP informs A-AgentiM that registration
975
          was successful.
976
977
       (inform
978
         :sender
979
           (agent-identifier
980
             :name df@gateway.com)
981
         :receiver (set
982
           (agent-identifier
983
             :name A-AgentiM@mobile.com))
984
         :language FIPA-SL0
985
         :protocol FIPA-Request
986
         :ontology FIPA-Agent-Management
987
         :content
988
           (done
989
             (action
990
                (agent-identifier :name df@gateway.com)
991
             (register
992
               (df-agent-description
993
                  :name
994
                    (agent-identifier
995
                      :name A-AgentiM@mobile.com
996
                      :addresses (sequence iiop://gateway.com/acc wap://mobile.com:1234/acc))
997
                  :services
998
                    (service-description (set
999
                      :name Field-Warrior
1000
                      :type field-information
1001
                      :ontology field-service
```

1002	:properties (set	
1003	(property	
1004	:name availability	
1005	:value 24h))))	
1006	<pre>:language (set FIPA-SL0))))</pre>	
1007		

Message 7 request, message 8 agree and message 9 inform: When A-AgentiM needs the Field-Warrior service, it searches the gateway host DF which informs it that A-AgentiM offers such a service (see [FIPA00023]).

# Message 10, 11, 12 and 13: The messages used and the message flow are similar to the example in Section 5.4.1, Message Exchange Activation by an Agent in a Mobile Host.

- 1013
- 1014

# 1014 6 Informative Annex A — Paramedic Scenario

1015 This section illustrates some of the important issues of nomadic application support, using a paramedic application as 1016 an example.

1017

1022

1024

1026

1030

1032

1034

1036

1038

#### 1018 6.1 Overview

- 1019 A paramedic team has several working environments: 1020
- 1021 An emergency dispatch centre, which is covered by the hospital ATM network,
- 1023 A geographical area, which is wireless wide-area network (e.g. GPRS), and,
- 1025 One or more hospitals, which are provided with a wireless local-area network.

1027 When in transit, the paramedic computers are attached to docking stations residing in ambulances. At the dispatch 1028 centre, the docking stations are connected to the ATM network. The paramedic application comprises the following 1029 services:

- 1031 Retrieval of a patient's personal information, such as name, address, phone, and relatives,
- 1033 Retrieval of the patient's medical histories,
- 1035 Support for paramedic workers, and,
- 1037 Informing the hospital receiving the patient about the patient's current injury or illness and medical care given so far.

1039 There are several application agents: Paramedic Support Agents (PSAs) working in the paramedic computers, 1040 Dispatching Support Agent (DSA) working at the dispatch centre system, and the Hospital First Aid Support Agent 1041 (HFASA) working at the hospital system.

1041 (HFA 1042 1043 The (

The dispatch centre receives a call regarding a man who has severe chest pain; the symptom of an acute myocardial 1044 infarct. The caller identifies the man and gives his personal identification number to the dispatcher. The dispatcher 1045 alerts the paramedic team and informs the DSA about the address where the patient is located and his personal 1046 identification number. The DSA simultaneously informs the PSA about the address of the attack (and possibly some 1047 additional information about the environment of the heart attack) and queries the patient's medical history. Since the 1048 results of the query to a local hospital are received before the paramedic unit is dispatched, the DSA (in co-operation 1049 with the PSA) begins to load the patient's personal information and medical history into the paramedic computers. The 1050 medical history includes several items of text-based information. The transmission time to load the information via the 1051 ATM network to the paramedic computers (which are currently docked at the dispatch centre) is less than a second. 1052 Before the ambulance leaves the dispatch centre, the docking station is detached from the ATM network and is 1053 connected to the wireless wide-area network. 1054

1055 While the ambulance is approaching the location of the incident, the DSA receives more relevant results of the query of 1056 the medical histories such as the latest heart operation of the patient. The medical history comprises several parts of 1057 textual information and several images and the DSA begins loading the information. As the loading takes place when 1058 the ambulance is in motion, the DSA finds out that the quality of transport service is too low for loading some textual 1059 parts and any of the images of the medical history. It would take at least 40 minutes to download the images. Therefore, 1060 the DSA informs the PSA that images are not required for the paramedic unit. During downloading, the ambulance 1061 drives into a tunnel that causes the wireless link to be disconnected. After the tunnel, a CA re-establishes the 1062 connection and downloading continues.

1063

At the scene, the ambulance is stationary and the quality of transmission service increases to a level at which the DSA is able to load the most relevant images (the ECGs) using an efficient compression method which is negotiated

between the DSA and the PSA to the paramedic computer. The paramedic team detaches the computers from the
 docking station and carries them to the patient.

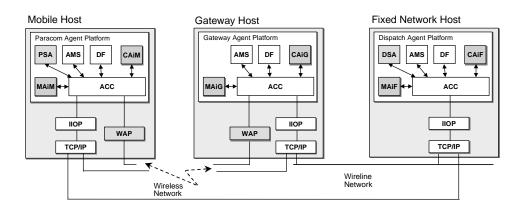
1069 The paramedic team realises that they need the assistance of a medical expert located at the university hospital to 1070 stabilise the patient's condition. Therefore, they attach electrodes to the patient and the PSA starts transmitting the data 1071 of measurement such as SpO2 (oxygen saturation), cardiac rhythm, ECG, end tidal CO2 and temperature to the 1072 hospital. After successfully stabilising the patient's condition, the paramedic team moves the patient to the ambulance 1073 and sets off for the hospital. As the quality of the transport service decreases because of the motion, the PSA finds out 1074 that not all the on-going measurement data can be transmitted on-line to the hospital. Therefore, the PSA decides to 1075 transmit the most relevant data (SpO2 and cardiac rhythm). The PSA stores the rest of the data (ECG, end tidal CO2 1076 and temperature) into a cache of the paramedic computer.

1077

After the ambulance arrives at the hospital, the patient is transferred immediately to an operating room. Simultaneously, the paramedic team connects their paramedic computer to the wireless LAN of the hospital and the PSA transmits (in co-operation with the HFASA) all the measurement data to the hospital's system. A surgeon retrieves and analyses the measurement data before surgery.

1082

This example illustrates a future agent-based distributed system that offers its services at the best obtainable quality of service in a wide variety of environments. A possible agent architecture is illustrated in *Figure 8* which refers to three separate APs: *Dispatch, Gateway* and *Paracom*. In addition, there are several hospital APs which are not illustrated.



1087 1088

1089

1090

1092

1094

Figure 8: Paramedic Scenario Architecture

- 1091 The agents in the scenario are:
- 1093 MAIM, MAIG and MAIF are MAs which monitor the quality of the communication service,
- 1095 CAIM, CAIG and CAIF are CAs which manage the establishment, teardown, suspension, activation, etc. of the 1096 connection between the PAs. The MA informs application agents about the status and changes of the network 1097 services. 1098
- When the mobile host is connected either to the ATM network or to the wireless LAN, the fipa.mts.mtp.iiop.std MTP is used directly between the *Paracom* AP and the *Dispatch* AP. When the mobile host is connected to the wireless WAN, all agent message communication takes place through the gateway host. The fipa.mts.mtp.wap.std MTP is primarily used between the *Paracom* AP and the *Gateway* AP. The fipa.mts.mtp.iiop.std MTP is used between the *Gateway* AP and the *Dispatch* AP.
- 1104
- 1105

#### 1105 6.2 Seamless Roaming

1106 The Seamless Roaming scenario describes the process, when the paramedic computer roams from the ATM network 1107 to the UMTS network. The scenario is split into following events:

- 1109 Disconnection and reconnection of MTCs,
- 1111 Negotiation of MTPs, and,
- 1113 Negotiation of message representations.
- 1114

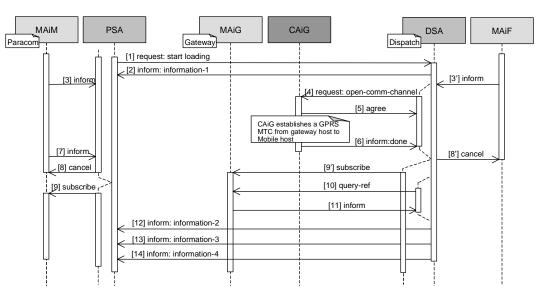
1108

1110

1112

#### 1115 6.2.1 Disconnection and Reconnection of an Message Transport Connection

- 1116 The message exchange between the agents is illustrated in *Figure 9*.
- 1117



1118 1119

1120

- Figure 9: Disconnection and Reconnection of an Message Transport Connection
- 1122 1. Message 1 request: The PSA starts loading data from the DSA by sending a request message. This message is 1123 application specific and thus not shown here.
- 1124 2. Message 2 inform: The DSA starts sending information by first sending an inform message.
- 1125 3. Messages 3 and 3' inform: MAiM (/ MAiF) informs the PSA (/DSA) that the ATM connection has broken.

```
1126
1127
       (inform
1128
         :sender
1129
           (agent-identifier
1130
             :name MAiM@paracom.com)
1131
         :receiver (set
1132
           (agent-identifier
1133
             :name PSA@paracom.com))
1134
         :ontology FIPA-Nomadic-Application
1135
         :language FIPA-SL2
1136
         :protocol FIPA-Subscribe
1137
         :content
1138
           (= (iota ?x
1139
             (gos-information
1140
                (comm-channel
1141
                  :name ATM
```

```
1142
                  :target-addr iiop://dispatch.com/acc)
1143
              (qos
1144
                :status ?x)))
1145
           disconnected))
1146
1147
       4. Message 4 request: The DSA requests CAiG to open a wireless wide-area MTC.
1148
1149
       (request
1150
         :sender
1151
           (agent-identifier
1152
              :name DSA@dispatch.com)
1153
         :receiver (set
1154
           (agent-identifier
1155
              :name CAiG@gateway.com))
1156
         :ontology FIPA-Nomadic-Application
1157
         :language FIPA-SL0
1158
         :protocol FIPA-Request
1159
         :content
1160
           (action
1161
              (agent-identifier
1162
                :name CAiG@gateway.com)
1163
              (open-comm-channel
1164
                (comm-channel
1165
                  :name GPRS
1166
                  :target-addr iiop://paramedic.com/acc))))
1167
1168
       5. Message 5 agree: CAiG agrees that it will try to open the GPRS connection.
1169
1170
       (agree
1171
         :sender
           (agent-identifier
1172
              :name CAiG@gateway.com)
1173
1174
         :receiver (set
1175
            (agent-identifier
1176
              :name DSA@dispatch.com))
1177
         :ontology FIPA-Nomadic-Application
1178
         :language FIPA-SL0
1179
         :protocol FIPA-Request
1180
         :content
1181
            ((action
1182
              (agent-identifier
1183
                :name CAiG@gateway.com)
1184
              (open-comm-channel
1185
                (comm-channel
1186
                  :name GPRS
1187
                  :target-addr iiop://paramedic.com/acc))))
1188
           true))
1189
1190
       Next CAIG establishes a GPRS MTC from the gateway host to the mobile host. This is an implementation issue.
1191
1192
       6. Message 6 inform: After successful establishment, CAiG informs the DSA.
1193
1194
       (inform
1195
         :sender
1196
            (agent-identifier
1197
              :name CAiG@gateway.com)
1198
         :receiver (set
1199
            (agent-identifier
1200
              :name DSA@dispatch.com))
1201
         :ontology FIPA-Nomadic-Application
1202
         :language FIPA-SL0
1203
         :protocol FIPA-Request
```

```
1204
         :content
1205
           (done
1206
             (action
1207
                (agent-identifier
1208
                  :name CAiG@gateway.com))
1209
              (open-comm-channel
1210
                (comm-channel
1211
                  :name GPRS
1212
                  :target-addr iiop://paramedic.com/acc))))
1213
1214
       7. Message 7 inform: MAiM informs the PSA that a new MTC has been established.
1215
1216
       (inform
1217
         :sender
1218
           (agent-identifier
1219
              :name MAiM@paracom.com)
1220
         :receiver (set
1221
           (agent-identifier
1222
              :name PSA@paracom.com))
1223
         :ontology FIPA-Nomadic-Application
1224
         :language FIPA-SL2
1225
         :protocol FIPA-Subscribe
1226
         :content
1227
           (= (iota ?x
1228
              (gos-information
1229
                (comm-channel
1230
                  :name GPRS
1231
                  :target-addr wap://paramedic.com:1234/acc)
1232
              (qos
1233
                :status ?x)))
1234
           connected))
1235
1236
       8. Message 8 and 8' cancel: The PSA (/DSA) cancels subscription notifications about the changes in the ATM MTC.
1237
1238
       (cancel
1239
         :sender
1240
           (agent-identifier
1241
             :name PSA@paracom.com)
1242
         :receiver (set
1243
           (agent-identifier
1244
              :name MAiM@paracom.com))
1245
         :ontology FIPA-Nomadic-Application
         :language FIPA-SL0
1246
1247
         :protocol FIPA-Subscribe
1248
         :content
1249
           (subscribe
1250
             :sender
1251
                (agent-identifier
1252
                  :name PSA@paracom.com)
1253
             :receiver (set
1254
                (agent-identifier
1255
                  :name MAiM@paracom.com))
1256
             :ontology FIPA-Nomadic-Application
1257
             :language FIPA-SL2
1258
              :protocol FIPA-Subscribe
1259
             :content
1260
                (iota ?x
                  (qos-information
1261
1262
                    (comm-channel
1263
                      :name GPRS
1264
                      :target-addr wap://paramedic.com:1234/acc)
1265
                    (qos
1266
                      :status ?x)))))
```

1268 9. Message 9 and 9' subscribe: The DSA (/PSA) subscribes to MAiG (/MAiM) for notifications about the changes in 1269 the GPRS MTC. 1270 1271 (subscribe 1272 :sender 1273 (agent-identifier 1274 :name DSA@dispatch.com) 1275 :receiver (set 1276 (agent-identifier 1277 :name MAiG@gateway.com)) 1278 :ontology FIPA-Nomadic-Application 1279 :language FIPA-SL2 1280 :protocol FIPA-Subscribe 1281 :content 1282 (iota ?x 1283 (gos-information 1284 (comm-channel 1285 :name GPRS 1286 :target-addr iiop://paramedic.com/acc) 1287 (qos 1288 :status ?x)))) 1289 1290 10. Message 10 query-ref: The DSA requests current quality of service of the GPRS MTC from MAIG. 1291 1292 (query-ref 1293 :sender 1294 (agent-identifier 1295 :name DSA@dispatch.com) 1296 :receiver (set 1297 (agent-identifier 1298 :name MAiG@gateway.com)) 1299 :ontology FIPA-Nomadic-Application 1300 :language FIPA-SL2 1301 :protocol FIPA-Query 1302 :content (iota ?x 1303 (qos-information 1304 1305 (comm-channel 1306 :name GPRS) 1307 (qos 1308 :throughput ?x))) 1309 1310 11. Message 11 inform: MAiG informs the DSA the current quality of service of the GPRS MTC. 1311 1312 (inform 1313 :sender 1314 (agent-identifier 1315 :name MAiG@gateway.com) 1316 :receiver (set 1317 (agent-identifier 1318 :name DSA@dispatch.com)) 1319 :ontology FIPA-Nomadic-Application 1320 :language FIPA-SL2 1321 :protocol FIPA-Query 1322 :content 1323 (= (iota ?x (qos-information 1324 1325 (comm-channel 1326 :name GPRS) 1327

```
      1327
      (qos

      1328
      :throughput ?x)))

      1329
      (rate-value
```

```
1330 :direction Outbound
```

- 1331
   :unit Kbits/s

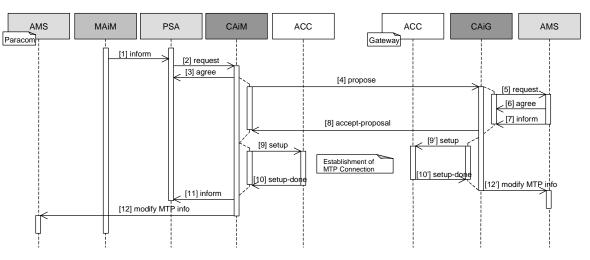
   1332
   :value 20)))
- 1333
- 1333 1334 1335

12. Messages 12, 13 and 14 inform: The DSA sends the rest of the requested information to the PSA.

#### 1336 6.2.2 Example Negotiation of a Message Transport Protocol

When the mobile host roams from the ATM network to the GPRS network – after the reconnection – the PSA receives the information from MAiM that the *Paracom* AP is now connected to the GPRS MTC. The PSA reasons that the fipa.mts.mtp.wap.std MTP is better in that environment and it requests the CAiM to establish this MTP between ACCIM and ACCIG. Also, CAIM proposes the establishment of this MTP to CAIG, which accepts the proposal, and they command their respective ACCs to set it up. As a last action, both CAIF and CAIG modify the AP descriptions of their APs. The message flow is illustrated in *Figure 10*.

1343



1344 1345 1346

1347

Figure 10: Example Negotiation of a Message Transport Protocol

1348 1. Message 1 inform: MAiM informs the PSA that the Paracom AP is now connected to the GPRS network.

```
1349
1350
       (inform
1351
         :sender
1352
           (agent-identifier
1353
              :name MAiM@paracom.com)
1354
         :receiver (set
1355
           (agent-identifier
1356
              :name PSA@paracom.com))
1357
         :ontology FIPA-Nomadic-Application
1358
         :language FIPA-SL2
1359
         :protocol FIPA-Subscribe
1360
         :content
1361
           (= (iota ?x)
1362
              (gos-information
1363
                (comm-channel
1364
                  :name GPRS
1365
                  :target-addr wap://paramedic.com:1234/acc)
1366
                (qos
1367
                  :status ?x)))
1368
           connected))
1369
1370
```

Message 2 request and message 3 agree: The PSA requests CAiM to establish the fipa.mts.mtp.wap.std
 MTP between ACCiM and ACCiG.

```
1372
1373
       (request
1374
         :sender
1375
           (agent-identifier
1376
              :name PSA@paracom.com)
1377
         :receiver (set
1378
           (agent-identifier
1379
              :name CAiM@paracom.com))
1380
         :ontology FIPA-Nomadic-Application
1381
         :language FIPA-SL0
1382
         :protocol FIPA-Request
1383
         :content
1384
           (action
1385
              (agent-identifier
1386
                :name CAiM@paracom.com)
1387
              (activate (sequence
1388
                (transport-protocol
1389
                  :name fipa.mts.mtp.wap.std
1390
                  :gw-addr wap://gateway.com:1234/acc))))
1391
1392
       3. Message 4 propose: CAIM sends a propose message to the CAIG.
1393
       (propose
1394
1395
         :sender
1396
           (agent-identifier
1397
             :name CAiM@paracom.com)
1398
         :receiver (set
           (agent-identifier
1399
1400
             :name CAiG@gateway.com))
1401
         :ontology FIPA-Nomadic-Application
1402
         :language FIPA-SL0
1403
         :protocol FIPA-Propose
1404
         :content
1405
           ((action
1406
              (agent-identifier
                :name CAiM@paracom.com)
1407
1408
              (use
1409
                (transports
1410
                  :send (sequence
1411
                    (transport-protocol
                      :name fipa.mts.mtp.wap.std))
1412
1413
                  :recv (sequence
1414
                    (transport-protocol
1415
                      :name fipa.mts.mtp.wap.std)))))
1416
           true))
1417
1418
       4. Message 5 request, message 6 agree and message 7 inform: CAiG requests the local AP description to find
1419
          out if the fipa.mts.mtp.wap.std MTP is supported (see [FIPA00023]).
```

1421 5. Message (8) accept-proposal: CAiG accepts CAiM's proposal to use the fipa.mts.mtp.wap.std MTP.

```
1422
1423
       (accept-proposal
1424
         :sender
1425
           (agent-identifier
1426
             :name CAiG@gateway.com)
1427
         :receiver (set
1428
           (agent-identifier
1429
             :name CAiM@paracom.com))
1430
         :ontology FIPA-Nomadic-Application
1431
         :language FIPA-SL0
1432
         :protocol FIPA-Propose
1433
         :content
1434
           (action
1435
             (agent-identifier
1436
               :name CAiM@paracom.com)
1437
             (use
1438
               (transports
1439
                 :send (sequence
1440
                    (transport-protocol
1441
                      :name fipa.mts.mtp.wap.std))
1442
                 :recv (sequence
1443
                    (transport-protocol
1444
                      :name fipa.mts.mtp.wap.std)))))
1445
           (transports
1446
             :send (sequence
1447
               (transport-protocol
1448
                  :name fipa.mts.mtp.wap.std))
1449
             :recv (sequence
1450
               (transport-protocol
1451
                  :name fipa.mts.mtp.wap.std))))
1452
1453
       6. Messages 9 and 9' setup and messages 10 and 10' setup-done: CAiM (CAiG) commands ACCiM (ACCiG) to
          setup the fipa.mts.mtp.wap.std MTP. As this is intra-platform communication between CAiM (CAiG) and
1454
1455
          ACCIM (ACCIG), this is an implementation issue.
1456
1457
       7. Message 11 inform: CAiM returns the result to the PSA.
1458
1459
       (inform
1460
         :sender
1461
           (agent-identifier
1462
             :name CAiM@paracom.com)
1463
         :receiver (set
1464
           (agent-identifier
1465
             :name PSA@paracom.com))
1466
         :ontology FIPA-Nomadic-Application
1467
         :language FIPA-SL0
1468
         :protocol FIPA-Request
1469
         :content
1470
           (result
1471
             (action
1472
                (agent-identifier
1473
                  :name CAiM@paracom.com)
1474
             (activate (sequence
1475
               (transport-protocol
1476
                  :name fipa.mts.mtp.wap.std
1477
                  :gw-addr wap://gateway.com:1234/acc)))
1478
             (transport-protocol
1479
               :name fipa.mts.mtp.wap.std
1480
               :gw-addr wap://gateway.com:1234/acc)))
1481
```

DSA

- 1482 8. Message 12 and 12' set-description: CAiM (CAiG) modifies the AP description to show that the 1483 fipa.mts.mtp.wap.std is now active.
- 1484

#### 1485 6.2.3 Example Negotiation of a Message Representation

MAiM

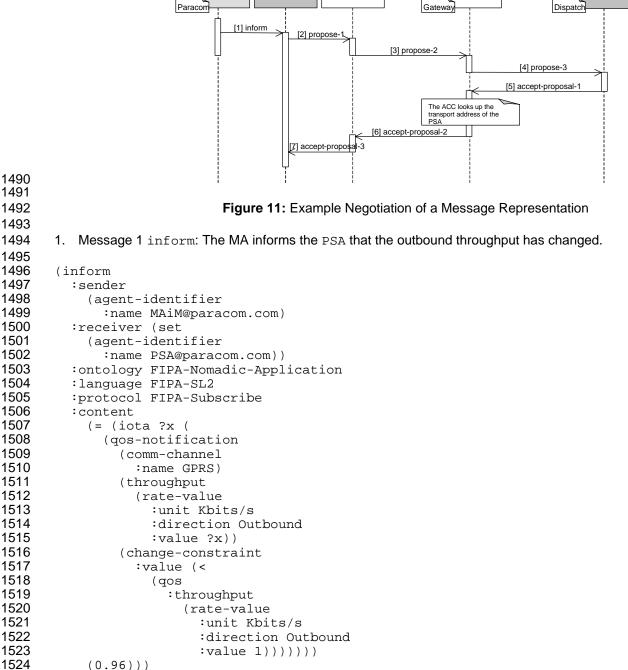
PSA

1486 MAIM informs the PSA that the quality of the message transport connection has dropped significantly. The PSA reasons 1487 that the ACL representation needs to be changed to fipa.acl.rep.bitefficient.std and it proposes that to the DSA. The DSA accepts the PSA's proposal. The message flow is illustrated in Figure 11. 1488

ACC

ACC

1489



(0.96)))

1525

1526 2. Message 2 propose-1: Based on the new throughput value, the PSA decides to change to the message 1527 representation. 1528

```
1528
1529
       (propose
1530
         :sender
1531
           (agent-identifier
1532
             :name PSA@paracom.com)
1533
         :receiver (set
1534
           (agent-identifier
1535
             :name DSA@dispatch.com))
1536
         :ontology FIPA-Message-Representation
1537
         :language FIPA-SL0
1538
         :protocol FIPA-Propose
1539
         :content
1540
           ((action
1541
             (agent-identifier
1542
                :name PSA@paracom.com)
1543
              (use
1544
                (msg-rep-selection
1545
                  :send (sequence
1546
                    (msg-representation
1547
                      :name fipa.acl.rep.bitefficient.std))
1548
                  :recv (sequence
1549
                    (msg-representation
1550
                      :name fipa.acl.rep.bitefficient.std)))))
1551
           true))
1552
1553
       3. Message 3 propose-2: The ACC at the mobile host forwards the same message to the ACC at the gateway host.
1554
       4. Message 4 propose-3: The ACC at the gateway host forwards the same message to the PSA.
1555
1556
1557
       5. Message 5 accept-proposal-1: The PSA accepts the proposal and sends a message back to the DSA.
1558
1559
       (accept-proposal
1560
         :sender
1561
           (agent-identifier
1562
             :name DSA@dispatch.com)
1563
         :receiver (set
1564
           (agent-identifier
1565
              :name PSA@paracom.com))
1566
         :ontology FIPA-Message-Representation
1567
         :language FIPA-SL0
1568
         :protocol FIPA-Propose
1569
         :content
1570
           (action
1571
              (agent-identifier
1572
                :name PSA@paracom.com)
1573
              (use
1574
                (msg-rep-selection
1575
                  :send (sequence
1576
                    (msg-representation
1577
                      :name fipa.acl.rep.bitefficient.std))
1578
                  :recv (sequence
1579
                    (msg-representation
1580
                      :name fipa.acl.rep.bitefficient.std))))
1581
              (msg-rep-selection
1582
                :send (sequence
1583
                  (msg-representation
1584
                    :name fipa.acl.rep.bitefficient.std))
1585
                :recv (sequence
1586
                  (msg-representation
1587
                    :name fipa.acl.rep.bitefficient.std)))))
1588
```

Message 6 accept-proposal-2: The ACC at the gateway host forwards same message to the ACC at the mobile host.

1591
1592 7. Message 7 accept-proposal-3: The ACC at the mobile host delivers the same message to the PSA.

# 1593 **7 References**

1594		
1595 1596	[FIPA00023]	FIPA Agent Management Specification. Foundation for Intelligent Physical Agents, 2000. http://www.fipa.org/specs/fipa00023/
1597 1598	[FIPA00027]	FIPA Query Interaction Protocol Specification. Foundation for Intelligent Physical Agents, 2000. http://www.fipa.org/specs/fipa00027/
1599 1600	[FIPA00035]	FIPA Subscribe Interaction Protocol Specification. Foundation for Intelligent Physical Agents, 2000. http://www.fipa.org/specs/fipa00035/
1601 1602	[FIPA00036]	FIPA Propose Interaction Protocol Specification. Foundation for Intelligent Physical Agents, 2000. http://www.fipa.org/specs/fipa00036/
1603 1604	[FIPA00069]	FIPA ACL Message Representation in Bit-Efficient Encoding Specification. Foundation for Intelligent Physical Agents, 2000.
1605		http://www.fipa.org/specs/fipa00069/
1606 1607	[FIPA00075]	FIPA Agent Message Transport Protocol for IIOP Specification. Foundation for Intelligent Physical Agents, 2000.
1608		http://www.fipa.org/specs/fipa00075/
1609 1610	[FIPA00076]	FIPA Agent Message Transport Protocol for WAP Specification. Foundation for Intelligent Physical Agents, 2000.
1611		http://www.fipa.org/specs/fipa00076/
1612 1613 1614	[ITUE800]	Recommendation E.800 - Telephone Network and ISDN, Quality of Service, Network Management and Traffic Engineering, Terms and Definitions Related to Quality of Service and Network Performance Including Dependability. International Telecommunication Union, International Telecommunication
1615		Union, 1995.
1616 1617 1618	[ITUX135]	Recommendation X.135 - Speed of Service (delay and throughput), Performance Values for Public Data Networks when Providing Packet-Switched Services. International Telegraph and Telephone Consultative Committee, 1993.
1619 1620	[WAP99]	Wireless Application Protocol Specification Version 1.2. WAP Forum, 1999. http://www.wapforum.org/what/technical.htm