# FOUNDATION FOR INTELLIGENT PHYSICAL AGENTS

# FIPA Network Management and Provisioning Specification

| | | | |
|---|---|---|---|
| **Document title** | FIPA Network Management and Provisioning Specification | | |
| **Document number** | PC00082 | **Document source** | FIPA Architecture Board |
| **Document status** | Preliminary | **Date of this status** | 2000/06/27 |
| **Supersedes** | OC00016 | | |
| **Contact** | fab@fipa.org | | |
| **Change history** | | | |
| 2000/06/27 | Carried forward from FIPA 1997 Specification 7 V1 | | |



*Geneva, Switzerland*

## 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 Scope

Across the world, numerous telecommunications service providers combine service elements from different network providers in order to provide a single service to end customers. The ultimate goal of all parties involved is to find the best solutions available in terms of quality of service and cost. The increasing demand for on-line customer configurable services and on-line provisioning of services requires systems and networks that are capable of co-operating on different levels and that transcend conventional business and national boundaries.

The dynamic Virtual Public Network (VPN) service is a telecommunications service provided to users that want to set up a multimedia connection with several other users. The provisioning of a dynamic VPN service is an example of how service providers and network providers will have to co-operate in order to provide this to the end-customer.

Traditional network management frameworks (for example, TMN or SNMP-based solutions) are based upon fixed management functionality and fixed interaction interfaces that cannot easily satisfy the flexibility and complexity that the dynamic multimedia VPN service demands. Agent technology is promising in this domain since it facilitates automatic negotiation of service contracts and subsequent configuration of those services, thus enhancing the provisioning process for the users and administrators of dynamic multimedia VPN services.

FIPA agents, which can interact using ACL, have significant advantages in this context. In summary FIPA agents can:

- Support effective negotiations that will be complex,
- Support dynamic service and service condition configuration via knowledge exchange,
- Reduce the dependency on the network reliability and availability by encapsulating the negotiation functionalities in ACL messages,
- Provide friendly and enhanced customer support via agency, and,
- Support personalization of the service resource configuration and utilisation using more detailed knowledge about users and providers and their preferences.

# 2 General Analysis

The VPN service provides a virtual private network over which multimedia applications can be executed. This specification does not specify the multimedia services or applications but they might be, for example, a virtual meeting, a shared workspace or a video conference. The VPN service is constructed, maintained and delivered using specialised co-operating and negotiating agents. This specification presents a scenario that is complex and realistic enough to exercise the feasibility of multi-agent technologies being proposed in FIPA; this document explores functional requirements and proposes a functional specification.

For actually provisioning the multimedia VPN service, three types of agents are used that represent the interests of the different parties involved (see *Figure 1*):

- **Personal Communications Agent (PCA)**
  This agent represents the interests of the human users.

- **Service Provider Agent (SPA)**
  This agent represents the interests of the service provider.

- **Network Provider Agent (NPA)**
  This agent represents the interests of the network provider.

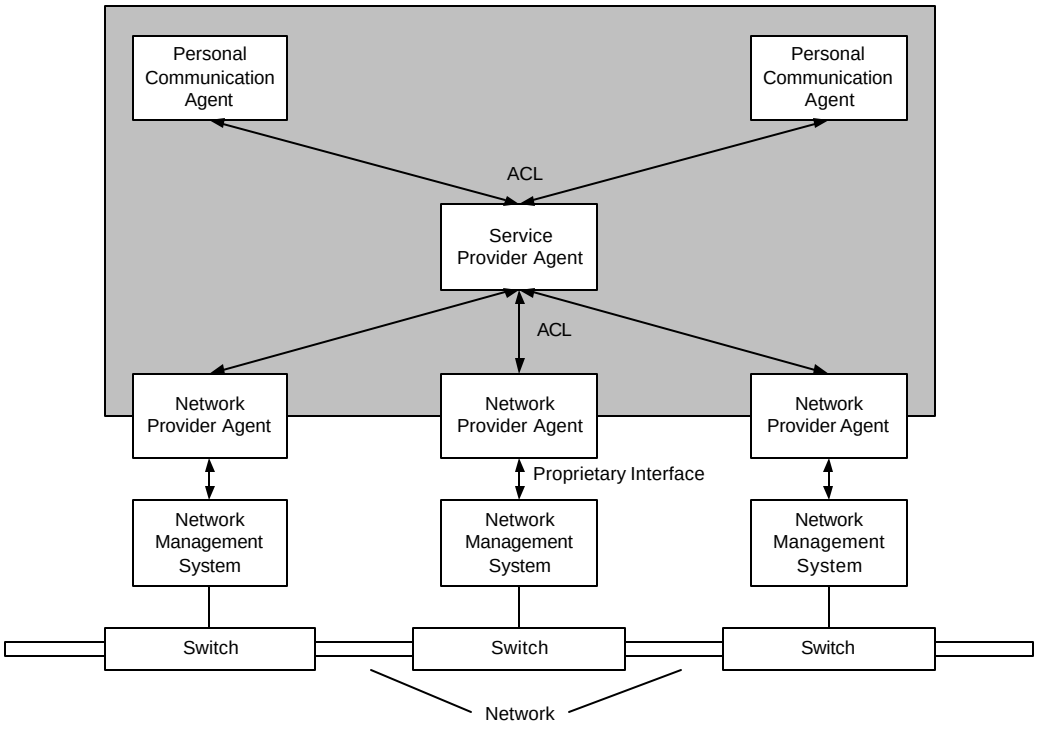


**Figure 1:** Virtual Public Network Multimedia Service Reference Model

For each type of network that will be used for the VPN service, it is necessary to provide a specialist agent that is able to translate requirements from the SPA to the appropriate network configuration settings.

The VPN service is established by the user who requests the service from their PCA, stating their requirements including the desired quality of service, cost constraints and duration. The initiating PCA negotiates with other PCAs to arrange preliminary conditions such as a time to start the service and terminal details; these initial communications will occur prior to the establishment of the VPN service using traditional network resources, such as the Internet. The initiating PCA will then negotiate with available SPAs to obtain the best service offer available and the SPA will in turn negotiate with

NPAs to obtain the optimal solution and to configure the service at the network level. Both SPAs and NPAs communicate with underlying service and network management systems to configure the networks for the service.

## 2.1 Functional Requirements

These requirements describe the high-level implementation-independent requirements for the dynamic VPN service. which are independent from the notion of an agent.

The following parties are involved in the provisioning of the dynamic VPN service and use their own negotiation strategies to meet their internal goals (neither of which will necessarily be publicly known):

- **User**
  The initiating user will negotiate with a service provider about the terms and conditions of the service to be provided at minimum cost. The receiving user will get a notification from the network provider that his participation is required in the VPN service when it has been established.

- **Service Provider**
  The service provider will negotiate with the user about terms and conditions as stated above. The service provider will also negotiate with its network provider in order to find the optimal solution for the provisioning of the service to the customer since the service provider has an interest in maximising its profit.

- **Network Provider**
  The network provider will negotiate with the service provider about terms and conditions as stated above and will also negotiate with other network providers for parts of the connection it cannot deliver itself or that can be offered more cheaply than the network provider can deliver since the network provider has an interest in maximising its profit. The network provider will notify the receiving customers that their participation is required once the VPN service has been established.

- **Third-Parties**
  Third-party network providers negotiate with the network provider to provide services. They will also notify the receiving customers once the VPN service has been established.

### 2.1.1 Initiating User Requirements

The dynamic VPN service is mainly aimed at the market segment represented by the executive traveller who is thought to be flexible, efficient and cost-effective. Further, the executive traveller expects a reliable, flexible service without being confronted with the technical implementation details.

The initiating user is responsible for the set up of the VPN service. When applying for provisioning of a dynamic VPN service, they must issue a request to the service provider in order to start the provisioning of the service. The requirements of the initiating user state what characteristics they will expect from the service.

Their requirements can be summarised as:

- Broadband Connection to Other Users (Mandatory)
  The VPN service shall support the provisioning of broadband connections to one or more other users. The underlying bearer network should make it possible to set up multimedia connections upon a user's request. For example, the user may request a semi-permanent ATM PVC connection.

- Anytime, Anyplace Connection (Mandatory)
  The VPN service shall have no restrictions for time and locality. The user can issue a request anywhere in the network at any time and the users to be connected can be located anywhere in the network. For example, the user may request the VPN service at 2am from a moving taxi using his GSM terminal to contact a local AP that resides in the base station of the mobile telephony operator.

- Dynamic Configuration (Mandatory)
  The service parameters (for example, quality of service, price, user list, bandwidth) and the number of participating users can be changed dynamically during the life-time of the VPN service. For example, the user may wish to change the bandwidth to allow video conferencing any time when the VPN service is active.

- Reliability (Mandatory)
  The VPN service shall be reliable in the sense that the agreed quality of service is met and that the risk of unexpected termination of the service is minimised. For example, all parties jointly providing the service have measures in place to guarantee 99% availability of the VPN service.

- Fault Tolerance (Mandatory)
  The VPN service should be robust in the sense that it can recover from most exceptions. For example, when a link that is part of the connection can no longer be provided because of a hardware fault, an alternative link is automatically invoked to keep the connection alive.

- Security Levels (Mandatory)
  The VPN service shall support different levels of security (authentication, non-repudiation, integrity, trust and confidentiality). For example, an unauthorised user who wants to use an established VPN service should be informed that they are not a valid member of the user list.

- Online Billing (Optional)
  The VPN service should be able to make billing information available on-line in real-time. For example, the user decides to change bandwidth and is informed that this cannot be done within their current budget.

- Intelligent and Flexible Customer Care (Optional)
  The VPN service should provide enhanced customer support such as delivering intelligent responses on requests about the provisioned service. For example, the user wants to know how much it will cost to add more participants to the service.

### 2.1.2 Receiving User requirements

The requirements of the receiving user can be summarised as:

- User Notification for Receiving Calls (Mandatory)
  The VPN service shall notify the user whenever a call is received for participation. For example, a user is requested to join the VPN.

- User Notification for Terminating Calls (Mandatory)
  The VPN service shall notify the user whenever the VPN service is terminated upon request of the initiating user. For example, the video meeting draws to a close.

- User Notification for Exceptions (Mandatory)
  The VPN service shall notify the user whenever an exception occurs that hampers the VPN service. For example, a hardware fault prevents a user from continuing participation.

### 2.1.3 Service Provider Requirements

During the life-time of the VPN service, service providers will be able to renegotiate contracts with network providers in order to further optimise the service that is delivered to the user. The dynamic renegotiation and reconfiguration should be invisible to the user.

- Profit Maximisation (Mandatory)
  The VPN service will allow the service provider to maximise their profit which means that the service provider has a negotiation strategy that maximises revenue and minimises cost for the deployment of the service. Negotiations will be undertaken within the constraints of required quality of service and cost as they are specified by the user.

- Negotiate Position with a User (Mandatory)
  The VPN service will allow the service provider to effectively negotiate about terms and conditions and the cost of the service with the user which results in a contractual agreement between the service provider and the user.

- Negotiate Position with a Network Provider (Mandatory)
  The VPN service will allow the service provider to effectively negotiate about terms and conditions and the cost of the service with the network provider which will results in a contractual agreement between the service provider and the network provider.

- User Satisfaction (Mandatory)
  The VPN service will allow the service provider to be able to satisfy the requirements of the user during the entire life-time of the service. This requirement implies that the VPN service allows the service provider to dynamically change their network providers.

#### 2.1.4 Third-Party Requirements

The requirements of third-party network providers can be summarised as:

- Profit Maximisation (Mandatory)
  The VPN service will allow the network provider to maximise their profit which means that the network provider has a negotiation strategy that maximises revenue and minimises cost for the deployment of the service. Negotiations will be undertaken within the constraints of required quality of service and cost as they are specified by the service provider.

- Negotiate Position with a Network Provider (Mandatory)
  The VPN service will allow the network provider to effectively negotiate about terms and conditions and the cost of the service with the service provider which will results in a contractual agreement between the network provider and the service provider.

### 2.2 Benefits

Current VPN services have been implemented in different application contexts and with different technologies. The agent-based approach advocated by this specification, has a number of advantages over existing technologies for the provisioning of dynamic VPN services.

#### 2.2.1 Satisfying Dynamic Virtual Public Network Provisioning

The major high-level requirements of the roles and actors in the VPN service are the capabilities to negotiate about service conditions and configurations and to notify (or be notified) accordingly. Service negotiation in this context will have the following objectives:

- The satisfaction of the requirements from users/customers, and,

- The optimisation of the service conditions and configurations, for example, minimal costs, maximum profits, etc.

With traditional negotiation mechanisms, for example, CMIP/SNMP-based service subscriptions, a user can only select the service features offered by the service provider. The interface between the negotiation partners is fixed by, for example, GDMO, IDL or ODL specifications. A user can only modify the service parameters if such modifications are allowed in the interface specification and thus the possibility of dynamically optimising the service conditions and configurations is limited.

FIPA agents, using ACL as the agent communication language, can significantly enhance the possibility of dynamic negotiation and optimisation. For example:

1. The service provider can change the knowledge (or inform such changes) of the user (for example, the customer care component at the user site) about the service provisioning. In this way, the service provider can dynamically change the form of the service features or even the service itself in response to new user or service provider requirements.

2. The user can express their wishes and preferences, inform the provider about new requirements and request new service features. With such information, the service provider can infer user characteristics and offer appropriate support.

3. Service negotiation can have several phases following a contract net protocol in order to reach the optimal agreement between the involved parties.

4. The involved parties can modify their negotiation strategy dynamically, depending on the intermediate negotiation results.

Therefore, FIPA agents provide a highly flexible, robust and user-friendly framework for service negotiations.

### 2.2.2 Satisfying the User Requirements

- Broadband Connection to Other Users
  Provisioning of connections can be affected by many quality of service parameters and FIPA agents can provide enhanced support for negotiating such parameters, resulting in a very flexible and user-oriented provisioning.

- Anytime, Anyplace Connection
  With FIPA agents, the requests and preferences of the users can be coded in ACL messages which can be sent to the responsible service provider. Large grain messages in this context can direct and determine the service features to be provisioned. The user can send the message from anywhere in the network and can even disconnect itself from the network after sending the message.

- Dynamic Configuration
  ACL communication between agents enables the reconfiguration of and agent's knowledge about service configuration and the corresponding functionalities and, therefore, the dynamic configuration of the service resources.

- Reliability and Fault Tolerance
  Negotiation that is based on ACL can treat exceptional situations more intelligently and support negotiations that are more robust. Using composite messages, like mobile agents, the encapsulation of the negotiation steps or management actions within the messages can be achieved. With such encapsulation, the number of messages transmitted over the network can be reduced and the dependency of VPN provisioning on the underlying remote network for management traffic can thus be lessened. This can further increase the reliability and fault tolerance of the provisioned service.

- On line Billing
  Via ACL-based service negotiations, the user can request and determine the specific billing features and ask the service provider to make the data available at requested schedules and patterns.

- Security Levels
  The user can negotiate with the service provider about the levels of the security for all the management operations.

- Intelligent and Flexible Customer Care
  This will be the most important feature supported by the FIPA agents.

### 2.2.3 Satisfying Receiving User Requirements

The receiving users will be notified of VPN service-related events via ACL messages.

### 2.2.4 Satisfying Service Provider Requirements

- Profit Maximisation
  This entails the optimisation of the resource usage based on the knowledge about user preferences and requirements. Such optimisation requires intelligent planning within the service provider by reasoning about the knowledge concerning the users. Sophisticated negotiation using ACL will be necessary to obtain such knowledge.

- Negotiate Position with a User
  This will be supported by ACL messages and the corresponding contract net protocol.

- Negotiate Position with a Network Provider
  Similar to the previous point.

- User Satisfaction
  The FIPA agent-based approach allows the provider to dynamically configure the service features to meet the user requirements.

### 2.2.5 Satisfying Third-Party Requirements

This is similar to section *2.2.4, Satisfying Service Provider Requirements*.

## 2.3 Actors, Roles and Domains

### 2.3.1 Generic Model

The Personal Communication Agent (PCA) acts as a Personal Assistant (PA) to the user and will typically reside on a PDA or a portable computer. Since the assumption is that the user is mobile, the PCA will have to register with an AP in order to obtain access to the Message Transport Service (see [FIPA00067]) in this new environment.

In order to obtain the VPN service, the PCA will negotiate with one or more Service Provider Agents (SPAs). Each SPA can be seen as the front-end of a network provider. In order to obtain relevant customer data, the SPAs might access existing Customer Care Systems (CCS).

Each SPA will now start to negotiate deals with different Network Provider Agents (NPAs) that each represent telecommunications networks or parts of them. The NPAs translate the high-level PCA requests into low-level technical requirements. In order to find out whether it can deliver the required service, each NPA will contact existing Network Management Systems (NMS) which are also represented by agents.

Some termination points of the requested VPN service might lie outside the network of the first network provider. If this is the case, then the NPA will contact peer NPAs with a request to supply the missing connections in order to configure the service. NPAs that provide connections to end users will contact the appropriate SPAs in order to negotiate over the delivery conditions.

### 2.3.2 Personal Communication Agent

The PCA represents the customer in its dealings with service providers and must elicit user requirements for a request for service. For example, a user wishes to set up an on-demand VPN service to a set of company executives so that an interactive meeting can take place. These company executives are located around the globe and so the VPN service will span a number of different networks and network types. It is assumed that information about user requirements already resides within the PCA. The PCA must maintain this information so that the user could be offered alternatives in the event that no ideal service offering is available.

To obtain the desired service with the stated constraints and preferences, the PCA must find and interact with SPAs. The negotiation between the PCA and the SPA can be thought of as iterated bargaining, where the PCS will employ a strategy for bargaining with SPAs so that it can realise its preferences.

In order to communicate with other agents, the PCA must register with an AP which provides directory facilities and, if necessary, gives access to additional resources such as video screens, etc.

If an SPA offers a service which is acceptable to the PCA, then it will accept the service. This acceptance will mean that the PCA will commit the necessary resources of it the user's company to provision the service. Similarly, the SPA will commit necessary resources that it needs, possibly by bargaining with other agents. Activation of the agree service follows and the PCA will terminate its bargaining with other SPAs for that particular service.

### 2.3.3 Service Provider Agent

The SPA represents the interests of the service provider and supports the provisioning of telecommunication services to users. It adopts two distinct roles:

1. As a client of network services offered by an NPA, and,

2. As a provider of a variety of telecommunication services to users via their PCA.

It is possible that this agent performs other management activities such as billing. At present, the SPA does not interact with other SPAs and as such does not act as a third-party provider.

The key functions performed by the SPA during service provisioning are as follows:

- Capture customer requirements and identify the service
  The SPA receives a service request from a PCA. The identification of customer service requirements might require iteration between SPA and PCA and negotiation over service characteristics. The SPA maps the PCA requirements onto an existing service portfolio.

- Determine component software and network service requirements
  The SPA decomposes the service request into its component services and software.

- Negotiate terms with the user as a provider
  The SPA interacts with the PCA in order to agree the terms and conditions of the delivery of the service.

- Identify secure NPAs for component services
  The SPA queries the DF for information on available NPAs for the delivery of component services.

- Negotiate with NPAs for component network services as a client
  The SPA has an understanding of the component services it requires and it also has a representation of the meta-knowledge concerning the negotiation, such as a negotiation strategy, a definition of acceptable terms defined as a dedicated ontology, a knowledge of the negotiating protocol and access external management systems.

In order for the SPA to provision a service to the PCA it requires access to a number of existing service management systems, for example, a customer entry system, a billing system, a customer credit check system, security management, etc. These might be non-agent systems with their own proprietary interfaces.

### 2.3.4 Network Provider Agent

The NPA represents a network domain. Its major responsibility is in the provisioning of network connectivity upon requests from the SPA. For this purpose, the NPA has to interact with the SPA representing the user, the network management system representing the local network domain and with other NPAs representing other network domains in the global environment.

To obtain a network connection from the NPA, the SPA will first negotiate with the associated NPA and inform it of the requirements on the connection. This negotiation can consider an already existing long-term contract between the two parties, but it has to support the specific requirements of the current session. The knowledge needed by the NPA in this interaction includes the service description knowledge and the in-service requirements.

To provide the requested connection, the NPA has to first breakdown the task into local connection segment reservations and external connection segments, based on some service strategy and knowledge about the global network environment. The NPA will then try to reserve connection segments in its local domain and segments through other NPAs to connect the terminating points.

For the task breakdown and for creating connection segment requests, the NPA will need a resource model for both the underlying network management system it represents and for the resource model of other network domains represented by the other NPAs. The NPA will also select the other NPAs based on an acquaintance model established via exchanging information among NPAs and DFs.

In its role as a third-party provider, the NPA must be able to negotiate with other NPAs over the requested sub-network connections.

### 2.3.5 Customer Care System

A Customer Care System (CCS) is a collective name for the facilities of the service provider supporting the provisioning of the service to the users. This can include a customer entry system, a billing system, a customer credit check system, etc. These are typically non-agent systems with their own proprietary interfaces which must be integrated with guidance from [FIPA00079].

### 2.3.6 Network Management System

A Network Management System (NMS) is the conventional (non-agent) network management software of the network domain. The NMS maintains a dynamic view of the network and is able to establish connections at the request of an NPA. Each NMS will be represented by exactly one NPA and these must be integrated with guidance from [FIPA00079].

### 2.3.7 Certification Server

A Certification Server is a trusted third-party that stores public keys for registered agents. These keys can be requested by any party wishing to validate the identity of such an agent.

## 2.4 System Requirements

### 2.4.1 Requirements for All Agents

These are the basic requirements that are relevant for the provisioning of the dynamic VPN service by the PCA, the SPAs and the NPAs:

- Negotiate Position
  The PCA, the SPAs and the NPAs shall be able to effectively negotiate about quality of service and cost. This means that they shall have sufficient information and intelligence to find an optimal solution within these constraints. For example, during the set up phase, the PCA requests a particular quality of the service from the SPA. The SPA cannot deliver this quality and the PCA suggests a lower quality for a lower price that still meets the quality requirements of the user.

- Traceability
  For the purpose of dynamic testing, the PCA, the SPAs and the NPAs shall be able to keep track of all their activities which involves timestamps, logs and reports about their activities upon request. For example, each agent keeps track of all its negotiation activities and sends the information to its HAP where a log is kept for later investigation.

- Reliability

The PCA, the SPAs and the NPAs shall be reliable in the sense that the risk of unexpected failure of the services offered by an agent is minimised. For example, a PCA should be capable of reconnecting itself with the MTS after the connection has been temporarily disabled.

- Fault Tolerance
  The VPN service should be robust in the sense that it can recover from most exceptions. For example, when a link that is part of the connection can no longer be provided because of a hardware fault in the switch, an alternative link is automatically installed to keep the connection established. An NPA will re-provision the link or acquire the link via a third-party NPA or report failure back to the SPA which will then try to re-provision the VPN using alternative network providers.

- Security Levels
  The PCA, the SPAs and the NPAs shall support different levels of security (authentication, non-repudiation, integrity and confidentiality). For example, when an agent that has not been authenticated tries to contact the SPA, it should be informed that it cannot have access to the services of the SPA.

### 2.4.2 Initiating PCA Requirements

- Interaction with SPAs
  The PCA shall be able to interact with an SPA in order to request the VPN service.

- Low User Complexity
  The PCA shall be able to establish and maintain the service without complicated interaction with the user. This implies that the PCA shall have enough intelligence to deal with unexpected situations or events as described in previous sections on reliability and fault tolerance. For example, during the life-time of the service, a link in the connection is no longer available. Without consulting the user, the PCA, in collaboration with SPAs and NPAs, should try to find an alternative link.

- Lowest Price Negotiation (Optional)
  The PCA may strive for the lowest possible price to be paid for the entire service. For example, during the set up of the VPN service, the PCA deals with various third-party providers and selects the cheapest solution without compromising the quality of the service as specified by the user.

- Optimum Performance Negotiation (Optional)
  The PCA may strive for the best possible performance for the entire service. For example, during the set up of the VPN service, the PCA deals with various third-party providers and selects the solution that offers highest quality without overspending the available budget.

### 2.4.3 Receiving PCA Requirements

- Reception of Call (Optional)
  The PCA may be able to receive and accept a call on behalf of its user. For example, if the PCA receives a message that involvement in a video conference is requested, then it will acknowledge the message and initiate the procedure to notify the user and to prepare the equipment.

- Interaction with Terminal Equipment (Optional)
  The PCA may be able to interact with terminal equipment such as a PC application that has video conferencing capabilities.

### 2.4.4 Requirements for the SPA

- Interaction with PCA
  The SPA shall be able to interact with a PCA, using a negotiation strategy that maximises its goals (e.g. maximum profit, maximum customer satisfaction).

- Interaction with NPA
  The SPA shall be able to interact with an NPA in order to inquire about the possibilities of supplying the service requested by the PCA, and in case of a successful bid, to establish the service. This implies that the SPA is capable of finding its default NPA that can provide the network service.

- Interface to Customer Care Systems
  The SPA shall be able to interface with the customer care systems in order to obtain information essential for its negotiation with the PCA. For example, the SPA is able to collect information about the requesting user for purposes of billing.

- Availability of Service Management Information (Optional)
  The SPA may be able to request and handle on-line and real-time service management information made available by the CCS of the service provider to support the fault tolerance aspects of the agents. For example, the SPA is able to produce information about the current status of the service upon request from a PCA.

- Online Billing (Optional)
  The SPA may be able to request and handle on-line and real-time billing information made available by the Service Provider. For example, the SPA is able to produce information about the running cost of the service upon request from a PCA.

### 2.4.5 Requirements for the NPA

- Interface to Third-Party NPAs
  The NPA shall be able to interface with third-party NPAs in order to establish the service that has been agreed upon with the SPA. This implies that the NPA is capable of finding third-party NPAs that can provide the network service in case the NPA cannot provide the network service itself. For example, an NPA is able to set up a connection between terminating points in the network using third-party network services.

- Interface to Network Management Systems
  The NPA shall be able to interface with the NMS of the network provider in order to establish and maintain the network service that has been agreed upon with the SPA. For example, an NPA is able to set up a connection between terminating points in the network.

- Ability to Handle NPA Requests
  The NPA shall be able to handle a request from another NPA to establish a connection to a termination point in its network.

# 3 Scenarios

This section explores the scenarios of the dynamic VPN service provisioning, using a use case approach. *Figure 2* illustrates the agents in the system and the key scenarios involved in the dynamic VPN provisioning application. The following sections illustrate the required interactions of the agents in each of these scenarios (each scenario draws on the `FIPA-VPN-Provisioning` ontology from section *5, Virtual Public Network Provisioning Ontology*)

Unless otherwise stated, the cardinality of an agent in the scenario is considered to be one. If the scenario suggests that potentially many agents of a particular type should take part in the dialogue, it is envisaged that the initiating agent composes separate ACL messages for each of the required destination agents.

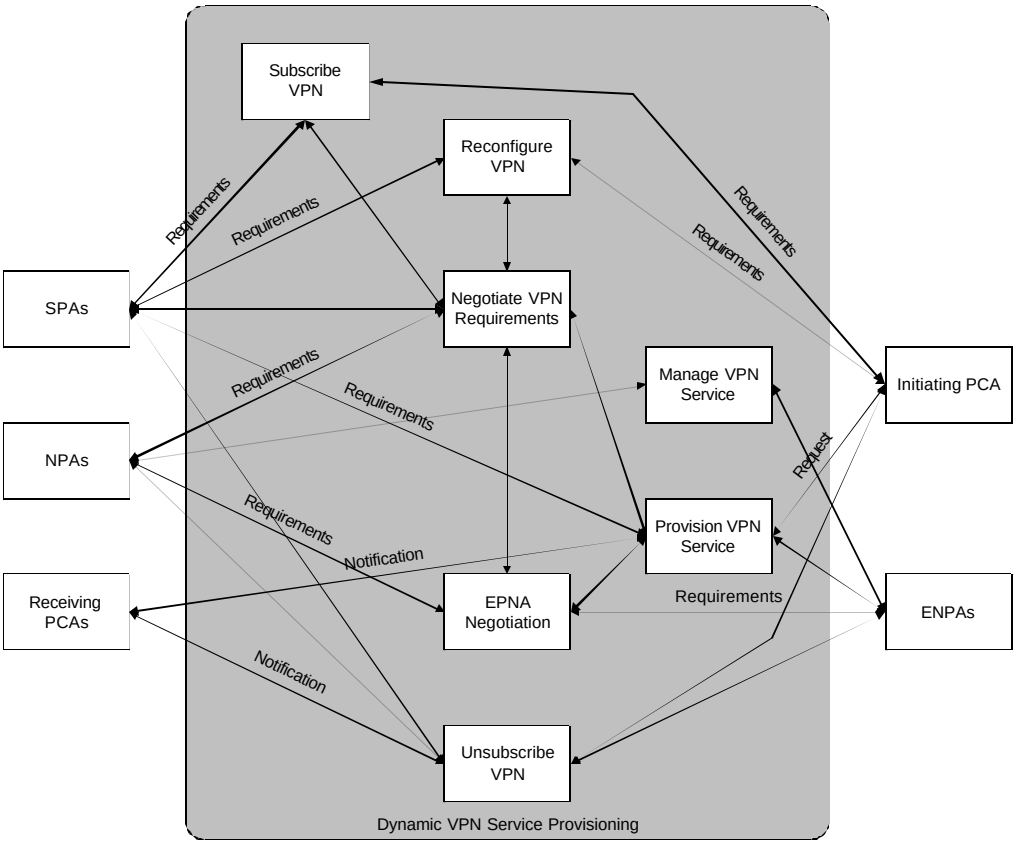


**Figure 2:** Multimedia VPN Service Provisioning Use Case Diagram

## 3.1 Subscribe Scenario

This scenario illustrates how the initiating PCA negotiates with one or more SPAs with an aim to establish a VPN service which best meets its requirements (see *Figure 3*).

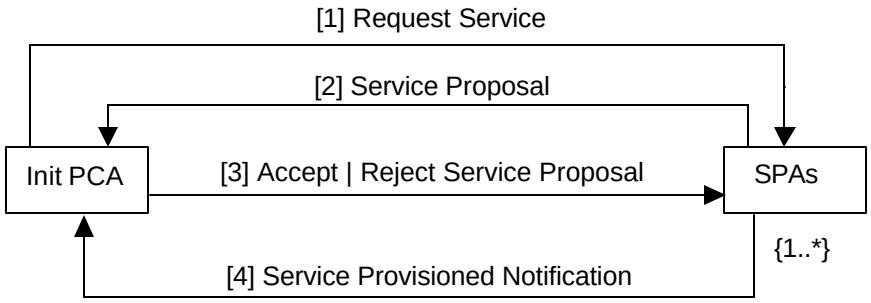


**Figure 3:** Service Subscription Collaboration

1. The initiating PCA sends a request service message to one or more SPAs:

```
(cfp
  :sender
    (agent-identifier
      :name InitPCA@foo.com
      :addresses (sequence iiop://foo.com/acc))
  :receiver (set
    (agent-identifier
      :name SPA1@bar.com
      :addresses (sequence iiop://bar.com/acc)))
  :ontology FIPA-VPN-Provisioning
  :protocol FIPA-Iterated-Contract-Net
  :language FIPA-SL0
  :content
     ((action
        (agent-identifier
          :name SPA1@bar.com
          :addresses (sequence (iiop://bar.com/acc))
      (establish
        (service-description
          :service-id Service1
          :service-type VideoOnDemand
          :user-ids (set User1 User2 User3)
          :respond-by ...)))
      true))
```

2. Each SPAs sends a service proposal message to the initiating PCA:

```
(propose
  :sender
    (agent-identifier
      :name SPA1@bar.com
      :addresses (sequence iiop://bar.com/acc))
  :receiver (set
    (agent-identifier
      :name InitPCA@foo.com
```

```
      :addresses (sequence iiop://foo.com/acc)))
  :ontology FIPA-VPN-Provisioning
  :protocol FIPA-Iterated-Contract-Net
  :language FIPA-SL0
  :content
     ((action
        (agent-identifier
          :name SPA1@bar.com
          :addresses (sequence (iiop://bar.com/acc))
      (establish
        (service-description
          :service-id Service1
          :service-type VideoOnDemand
          :user-ids (set User1 User2 User3)
          :respond-by ...))
     (establish
       (service-description
         :service-id Service1
         :service-type VideoOnDemand
         :user-ids (set User1 User2 User3)))
   :reply-with ServiceOffer1)
```

3. The initiating PCA sends accept or reject proposal message to the SPAs:

```
(accept-proposal
  :sender
    (agent-identifier
      :name InitPCA@foo.com
      :addresses (sequence iiop://foo.com/acc))
  :receiver (set
    (agent-identifier
      :name SPA1@bar.com
      :addresses (sequence iiop://bar.com/acc)))
  :ontology FIPA-VPN-Provisioning
  :protocol FIPA-Iterated-Contract-Net
  :language FIPA-SL0
  :content
     ((action
        (agent-identifier
          :name SPA1@bar.com
          :addresses (sequence (iiop://bar.com/acc))
      (establish
        (service-description
          :service-id Service1
          :service-type VideoOnDemand
          :user-ids (set User1 User2 User3)
          :respond-by ...))
    true)
  :reply-with ServiceAcceptance1
  :in-reply-to ServiceOffer1)
```

4. The accepted SPA sends a service provisioned notification message to the initiating PCA:

```
(inform
  :sender
    (agent-identifier
```

```
        :name SPA1@bar.com
        :addresses (sequence iiop://bar.com/acc))
    :receiver (set
      (agent-identifier
        :name InitPCA@foo.com
        :addresses (sequence iiop://foo.com/acc)))
    :ontology FIPA-VPN-Provisioning
    :protocol FIPA-Iterated-Contract-Net
    :language FIPA-SL0
    :content
       ((action
          (agent-identifier
            :name SPA1@bar.com
            :addresses (sequence (iiop://bar.com/acc))
         (establish
           (service-description
             :service-id Service1
             :service type VideoOnDemand
             :user-ids (set User1 User2 User3)
             :respond-by ...)))
       true))
```

## 3.2 Negotiate Requirements Scenario

This scenario illustrates how one of the selected SPAs prepares the service proposal for the initiating PCA from a number of NPAs (see *Figure 4*).

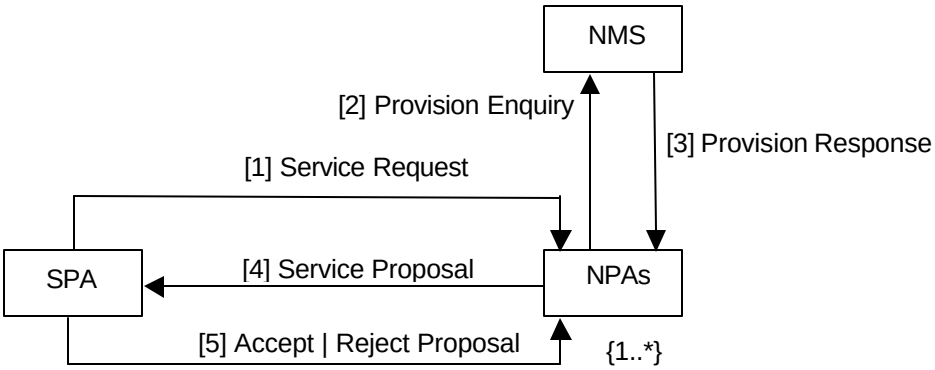


**Figure 4:** Service Negotiation Collaboration

1. The SPA sends a service request message to one ore more NPAs.
2. Each NPA sends a provision enquiry messages to its NMS Wrapper Agent (NMSWA).
3. Each NMSWA of an NPA sends a provision response to its NPA.
4. Each NPAs sends a service proposal messages to the SPA.
5. The SPA sends accept or reject proposal messages to the NPAs.

## 3.3 External Network Provider Agent Negotiation Scenario

This scenario illustrates how one of the selected NPAs attempts to find third-party External NPAs (ENPAs) which can provision the services that it cannot (see *Figure 5*).

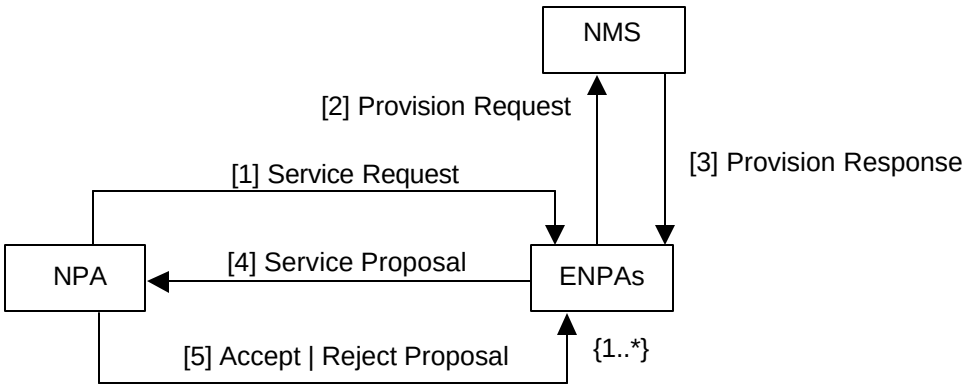


**Figure 5:** Third-Party Service Negotiation Collaboration

1. The NPA sends a service request message to one or more ENPAs.
2. Each ENPA sends a provision enquiry message to its NMSWA.
3. Each NMSWA of an ENPA sends a provision response to its ENPA.
4. Each ENPAs sends a service proposal messages to the NPA.
5. The NPA sends accept or reject proposal messages to the ENPAs.

## 3.4 Provision Service Scenario

This scenario illustrates how one of the selected NPAs actually provisions the required service (see *Figure 6*).

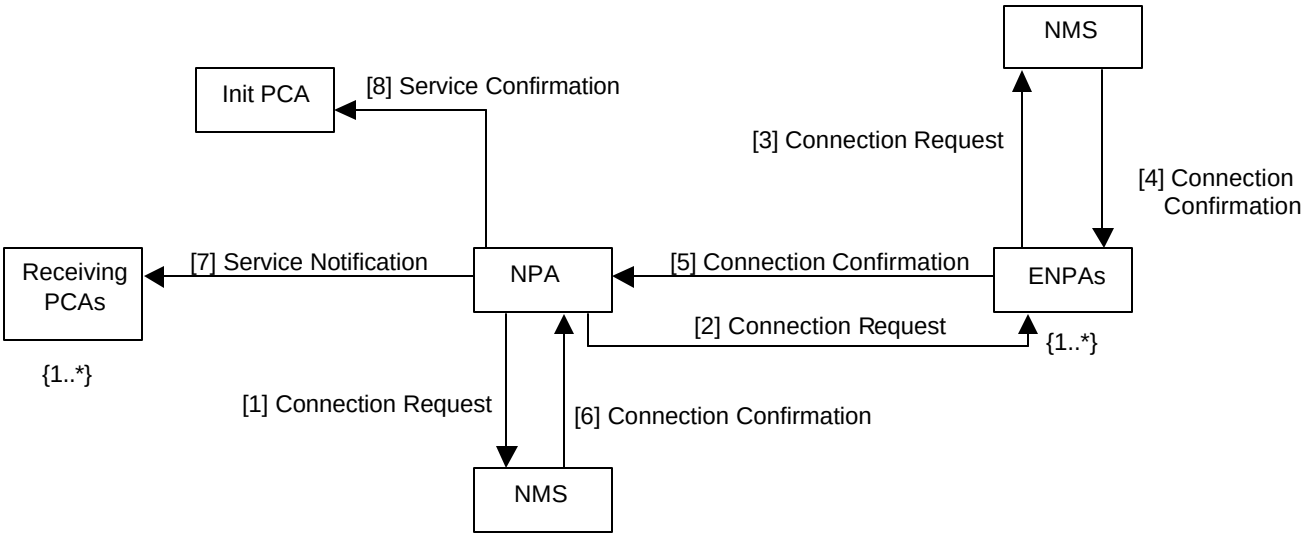


**Figure 6:** Service Provisioning Collaboration

1. The NPA sends a connection request message its NMSWA.

2. The NMSWA of the NPA sends a connection confirmation message to the NPA.
3. The NPA sends a connection request message to one or more ENPAs.
4. Each ENPA sends a connection request message to its NMSWA.
5. Each NMSWA of a ENPA sends a connection confirmation message to its ENPA.
6. Each ENPAs sends a connection confirmation messages to the NPA.
7. The NPA sends a service notification message to the receiving PCAs.
8. The NPA sends a service notification message to the initiating PCA.

## 3.5 Reconfigure Scenario

This scenario illustrates how the initiating PCA negotiates with one or more SPAs with the aim of altering the provisioned VPN service (see *Figure 7*).

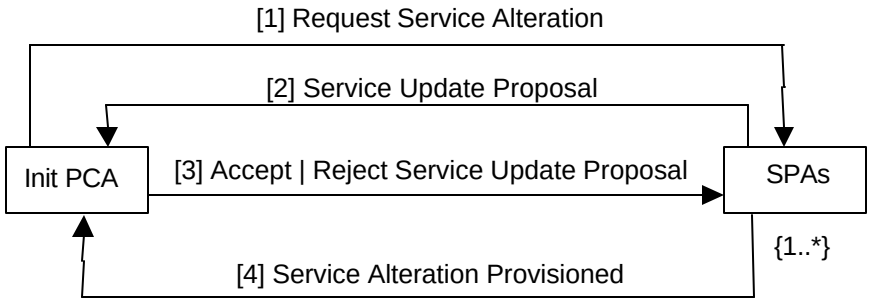


**Figure 7:** Service Reconfiguration Collaboration

1. The initiating PCA sends a request message service to one or more SPAs.
2. Each SPA sends a service proposal message to the initiating PCA.
3. The initiating PCA sends accept or reject proposal messages to the SPAs.
4. The accepted SPA sends a service provisioned notification message to the initiating PCA.

## 3.6 Manage Scenario

This scenario illustrates how the NPA monitors and maintains the VPN service: the management actions form part of the `FIPA-VPN-Management` ontology[1] (see *Figure 8*).

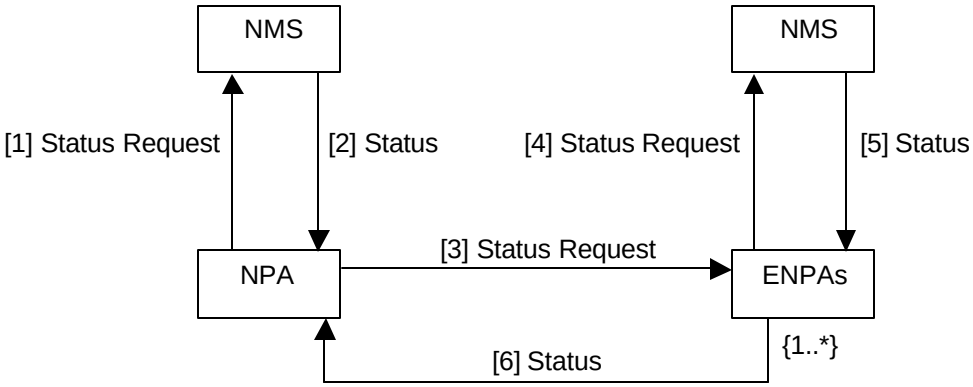


**Figure 8:** Service Management Collaboration

1. The NPA requests a network management status from its NMSWA.
2. The NMSWA sends a network management status message to its NPA.
3. The NPA requests a network management status from one or more ENPAs.
4. Each ENPA sends a network management status request message to its NMSWA.

[1] Currently unspecified.

5. Each NMSWA of an ENPA sends a network management status message to its ENPA.

6. Each ENPAs sends a network management status messages to the NPA.

## 3.7 Unsubscribe Scenario

This scenario illustrates how the initiating PCA requests the established VPN service to be terminated (see *Figure 9*).

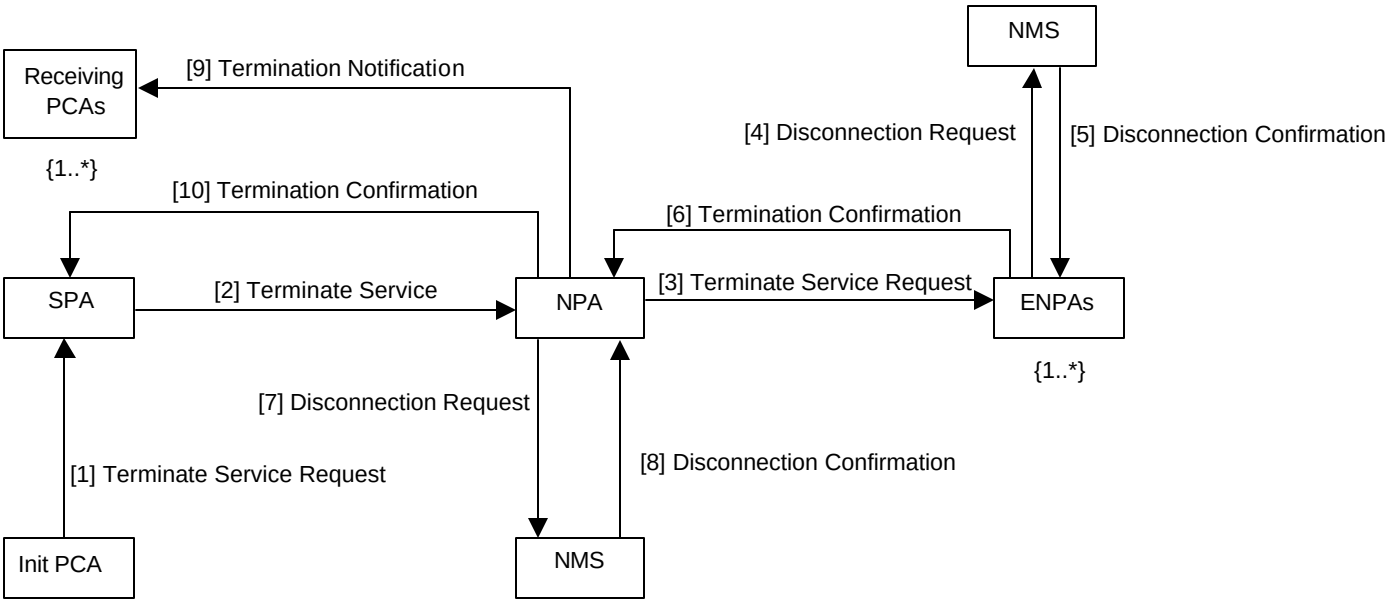


**Figure 9:** Service Unsubscription Collaboration

1. The initiating PCA sends a terminate service request message to the SPA.

2. The SPA sends a terminate service request message to one or more NPAs.

3. Each NPA sends a terminate service request message to its NMSWA.

4. Each NMSWA of an NPA sends a disconnect confirmation message to its NPA.

5. Each NPA sends a terminate service request message to one or more ENPAs.

6. Each ENPA sends a disconnect service request message to its NMSWA.

7. Each NMSWA of an ENPA sends a disconnect confirmation message to its ENPA.

8. Each ENPA sends a disconnect confirmation messages to the NPA.

9. Each NPA sends a termination notification message to the SPA.

10. The SPA sends a termination notification message to one or more receiving PCAs.

11. The SPA sends a termination notification message to the initiating PCA.

## 3.8 Generic Negotiation Scenario

Authentication will be required of all agents and APs and this scenario illustrates the required interactions for an arbitrary A to authenticate the arbitrary Agent B (see *Figure 10*).

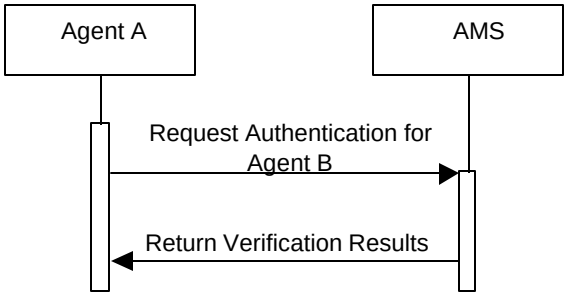


**Figure 10:** Generic Authentication Interaction

However, negotiation strategies (relating to agent goals) are internal to agents, and are not subject to standardisation in this document.

### 3.8.1 Basic Contract Net Protocol

The basic contract net protocol (see [FIPA00029]) is used between the PCA and the SPA and between the SPA and the NPA as illustrated in *Figure 11*. In the first case that is not really the contract net because the request-proposal is not multicasted. The general idea is to make a call for proposal and then to select one proposal. When an agent makes a proposal, it commits to achieve its proposal if it is accepted.

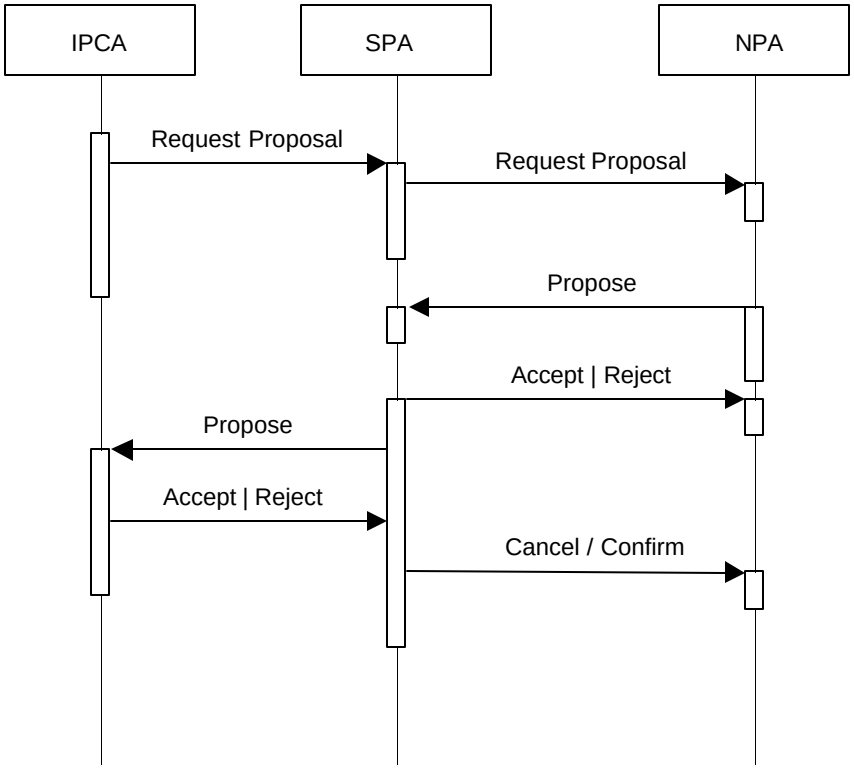


**Figure 11:** Basic Contract Net Protocol Interaction

Another version of this protocol could be designed in which the SPA can make a proposal to the PCA before consulting the NPAs by using its knowledge of previous experiences. In such a protocol the confirm/cancel request is sent to the initiating PCA by the SPA at the end of the scenario (after the reception and selection of all NPA's resources).

### 3.8.2 Iterated Contract Net Protocol

This protocol (see [FIPA00030]) is an extension of the basic contract net protocol but it includes a negotiation phase where the agents make counter proposals to find an agreement (see *Figure 12*). At the present time only the negotiation between the PCA and the SPA is considered.

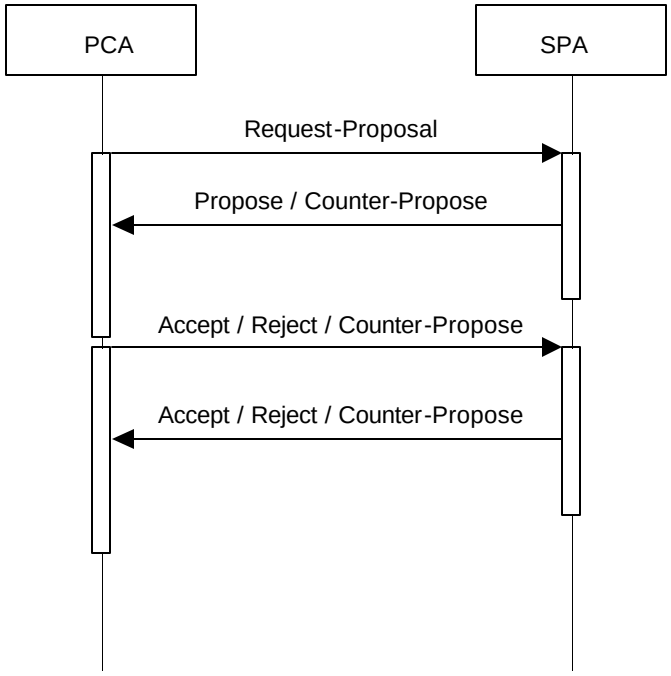


**Figure 12:** Iterated Contract Net Protocol Interaction

The interaction protocols for SPA to NPA and NPA to ENPA negotiation can be implemented in a similar way.

Example values to negotiate over could be:

- **Time, Date or Duration**
  The time, date and duration of the proposed service. This will be dependent on participating user's availability and preferences but will in turn be influenced by existing commitments of the network resources.

- **Quality of Service**
  This will reflect the user's requirements for the parameters of the VPN application, but will also be influenced by the availability of physical resources. It is reasonable to assume that in most cases a higher quality of service will incur a higher cost.

- **Security**
  The method and level of encryption used to secure the data being transferred during the service. Different service providers may be able to offer different methods or levels of encryption.

- **Cost**
  The cost to the service provider of buying the desired service from the network provider. This will be dependent on the above parameters.

- **Response Time**
  The time by which the requesting SPA expects a response from the recruited NPAs that a suitable service has been identified (and/or provisioned). The shorter the response time, the less scope there is for interaction between agents within the system. It is reasonable to assume that the longer the response time specified, the more suitable service the SPA will be able to identify/provision.

## 3.9 User Interaction Overview

It is envisaged that there would be three distinct phases of interaction between the user and his/her PCA. These interactions are illustrated in *Figure 13*.

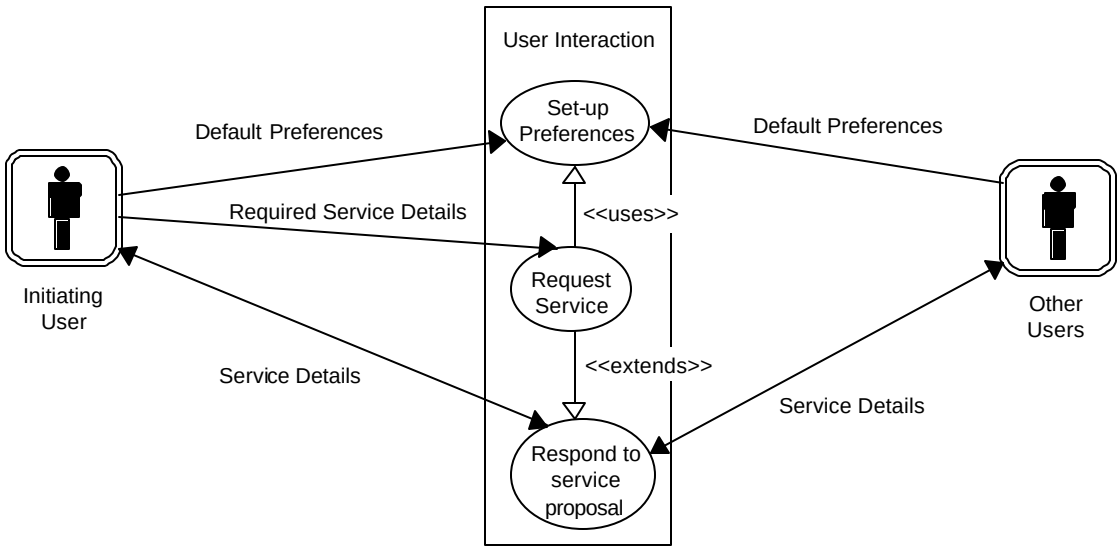


**Figure 13:** User and Personal Communication Agent Interaction

### 3.9.1 Setting Preferences

Before using the system for the first time, the user would configure their PCA with their preferences for certain parameters (for example, preferred applications, payment details etc.). The user's PCA would use these as default values when setting up services unless specifically instructed otherwise by the user. This information forms the basic knowledge which a PCA can use when it is approached by other PCAs.

### 3.9.2 Request a Service

When requesting a VPN service to be established between specific participants, the user would detail their PCA with information specific to that service, such as time, date, duration, security requirements, etc. He may choose to override his default preferences, for example to select a higher quality of service.

### 3.9.3 Respond to a Proposed Service

By this stage, the PCAs representing the users have carried out initial negotiations and information sharing (security requirements, for example,) and have composed a proposal for the service which is hopefully acceptable to all participants. The PCAs present this proposal to all participants for their approval and each participating user can then take one of three actions: accept the service proposal as described, reject the service proposal or modify the service proposal.

By accepting the proposal, the user indicates that he is satisfied for the service. Choosing to reject the proposal will terminate any future involvement of the user in the service (for example, it may no longer be relevant for the user to attend). If the user still desires to participate, but is not altogether satisfied with the details (maybe the proposed service

clashes with an appointment that is not stored in the user's diary), then the user can modify the service details, their diary or preferences appropriately and thus instruct their PCA to re-negotiate the service details.

The PCAs will agree alternative details and subsequently present these to the participants for their response. This process will continue until all involved participants accept the proposal or there are less than two participants still interested in attending the service.

# 4 High Level Information Model

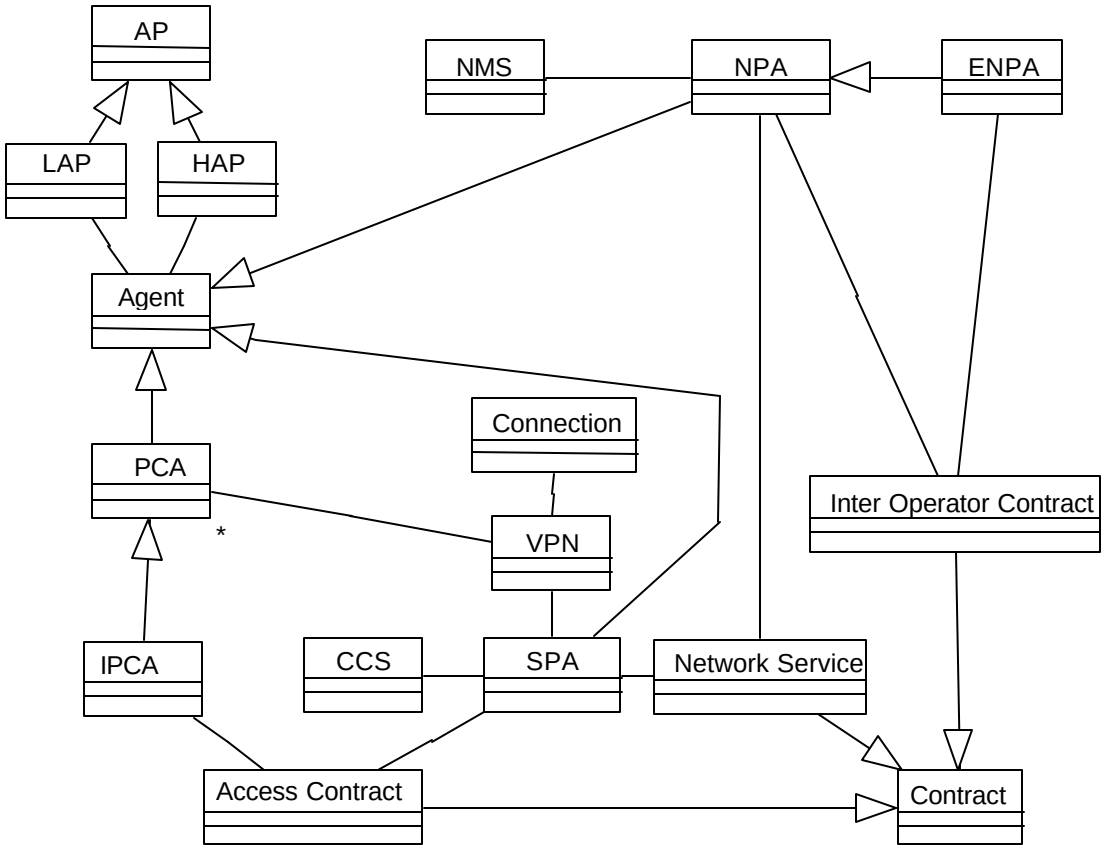


**Figure 14:** Virtual Public Network Class Overview

*Figure 14* shows a simple class overview (no attributes or methods have been defined) which shows the relationships between the main objects in the system:

- **Agents**
  These are the prime entities of the system which communicate and co-ordinate to achieve shared plans and to negotiate over the services to be delivered. To make this concrete, agents negotiate over the terms and conditions of contracts for service delivery.

  1. The PCA is the general class of personal communication agent which serves individual users,
  2. The initiating PCA is the PCA which initiates the dynamic VPN request,
  3. The SPA is the agent which provides the dynamic VPN service to the initiating PCA,
  4. The NPA is the agent which provides the network resources to realise the service, and,
  5. The ENPA is the agent which provides third-party network resources to realise the service.

- **APs**
  These represent the physical environments where agents reside.

  1. The home AP is where the agent was first created, and,

2. The local AP is where the agent currently resides.

- **Contracts**
  These are the informational items which the agents negotiate over and negotiation in this context means agreeing to the set of attributes contained in the contract:

  1. The *Access Contract* is the contract between the initiating PCA and the SPA,

  2. The *Network Service* is the contract between the SPA and the NPA, and,

  3. The *Inter Operator Contract* is the contract between the NPA and the ENPA.

- **Software Systems**
  These are the various software systems which are under direct control of their respective agents:

  1. The CCS is controlled by the SPA to initiate customer functions, and,

  2. The NMS is controlled by the NPA to reserve and manage network resources.

- **Connection**
  This is the class of service-level resources which are reserved by the NPA on behalf of the SPA in order to provide the dynamic VPN service.

# 5 Virtual Public Network Provisioning Ontology

## 5.1 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-VPN-Provisioning` ontology.

The following terms are used to describe the objects of the domain:

- **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.
- **Parameter**. This is the mandatory name of a parameter of this frame.
- **Description**. This is a natural language description of the semantics of each parameter.
- **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.

### 5.1.1 Service Description

This type of object represents the description of a VPN service.

| **Frame** | `service-description` | | | |
|---|---|---|---|---|
| **Ontology** | `FIPA-VPN-Provisioning` | | | |
| **Parameter** | **Description** | **Presence** | **Type** | **Reserved Values** |
| `service-type` | The type of the service. | Mandatory | `String` | |
| `service-id` | The identifier of the service. | Mandatory | `String` | |
| `user-ids` | A list of user identifiers using the service. | Optional | Set of `String` | |
| `security-level` | The security level that the users are allowed | Optional | `String` | |
| `respond-by` | The date and time by which replies to this service should be sent. | Optional | `DateTime` | See [FIPA00070] |
| `qos` | A list of quality of service requirements for the service. | Optional | Set of `String` | |

### 5.1.2 Service Connection

This type of object represents the description of a VPN service connection.

| **Frame Ontology** | `service-connection FIPA-VPN-Provisioning` | | | |
|---|---|---|---|---|
| **Parameter** | **Description** | **Presence** | **Type** | **Reserved Values** |
| `service-type` | The type of the connection. | Mandatory | `String` | |
| `connection-id` | The identifier of the connection. | Mandatory | `String` | |
| `contract-id` | The identifier of the contract associated with the connection. | Mandatory | `String` | |
| `security-level` | The security level that the users of the connection are allowed. | Optional | `String` | |
| `respond-by` | The date and time by which replies to this connection should be sent. | Optional | `DateTime` | |
| `qos` | A list of the quality of service associated with the connection. | Mandatory | Set of `String` | |

### 5.1.3 Video Description

This type of object represents a video service description.

| **Frame Ontology** | `video-description FIPA-VPN-Provisioning` | | | |
|---|---|---|---|---|
| **Parameter** | **Description** | **Presence** | **Type** | **Reserved Values** |
| `identifier` | The identifier of the video stream. | Mandatory | `String` | |
| `format` | The format of the video stream. | Mandatory | `String` | |
| `encryption` | The mechanism used to encrypt the video stream. | Mandatory | `String` | |

### 5.1.4 Voice Description

This type of object represents a voice service description.

| **Frame Ontology** | `voice-description FIPA-VPN-Provisioning` | | | |
|---|---|---|---|---|
| **Parameter** | **Description** | **Presence** | **Type** | **Reserved Values** |
| `identifier` | The identifier of the voice stream. | Mandatory | `String` | |
| `format` | The format of the voice stream. | Mandatory | `String` | |
| `encryption` | The mechanism used to encrypt the voice stream. | Mandatory | `String` | |

### 5.1.5 Data Description

This type of object represents a data service description.

| **Frame Ontology** | `data-description` `FIPA-VPN-Provisioning` | | | |
|---|---|---|---|---|
| **Parameter** | **Description** | **Presence** | **Type** | **Reserved Values** |
| `identifier` | The identifier of the data stream. | Mandatory | `String` | |
| `format` | The format of the data stream. | Mandatory | `String` | |
| `encryption` | The mechanism used to encrypt the data stream. | Mandatory | `String` | |

### 5.1.6 Video Conferencing Description

This type of object represents a video conferencing service description.

| **Frame Ontology** | `conferencing-description` `FIPA-VPN-Provisioning` | | | |
|---|---|---|---|---|
| **Parameter** | **Description** | **Presence** | **Type** | **Reserved Values** |
| `identifier` | The identifier of the conferencing stream. | Mandatory | `String` | |
| `format` | The format of the conferencing stream. | Mandatory | `String` | |
| `encryption` | The mechanism used to encrypt the conferencing stream. | Mandatory | `String` | |

## 5.2 Function Descriptions

The following tables define usage and semantics of the functions that are part of the `FIPA-VPN-Provisioning` ontology.

The following terms are used to describe the functions of the `FIPA-VPN-Provisioning` domain:

- **Function**. This is the symbol that identifies the function in the ontology.
- **Ontology**. This is the name of the ontology, whose domain of discourse includes the function described in the table.
- **Supported by**. This is the type of agent that supports this function.
- **Description**. This is a natural language description of the semantics of the function.
- **Domain**. This indicates the domain over which the function is defined. The arguments passed to the function 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 is a symbol belonging to the set identified by the range.
- **Arity**. This indicates the number of arguments that a function takes. If a function can take an arbitrary number of arguments, then its arity is undefined.

### 5.2.1 Establishing a Service with an Agent

| | |
|---|---|
| **Function** | `establish` |
| **Ontology** | `FIPA-VPN-Provisioning` |
| **Supported by** | PCA and SPA |
| **Description** | The execution of this function has the effect of establishing a new service. |
| **Domain** | `service-description` |
| **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 |

### 5.2.2 Modification of a Service with an Agent

| | |
|---|---|
| **Function** | `modify` |
| **Ontology** | `FIPA-VPN-Provisioning` |
| **Supported by** | PCA |
| **Description** | An agent may make a modification in order to change a service description. The argument of a `modify` function will replace the existing service description stored within the executing agent. |
| **Domain** | `service-description` |
| **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 |

### 5.2.3 Termination of a Service with an Agent

| | |
|---|---|
| **Function** | `terminate` |
| **Ontology** | `FIPA-VPN-Provisioning` |
| **Supported by** | SPA |
| **Description** | The execution of this function has the effect of terminating a service. |
| **Domain** | `service-description` |
| **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 |

### 5.2.4 Establishing a Service Connection with an Agent

| | |
|---|---|
| **Function** | `establish` |
| **Ontology** | `FIPA-VPN-Provisioning` |
| **Supported by** | NPA and NMSWA |
| **Description** | The execution of this function has the effect of establishing a new service connection. |
| **Domain** | `service-connection` |
| **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 |

### 5.2.5 Modification of a Service Connection with an Agent

| | |
|---|---|
| **Function** | `modify` |
| **Ontology** | `FIPA-VPN-Provisioning` |
| **Supported by** | NPA and NMSWA |
| **Description** | An agent may make a modification in order to change a service connection. The argument of a `modify` function will replace the existing service connection stored within the executing agent. |
| **Domain** | `service-connection` |
| **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 |

### 5.2.6 Roll-Back of a Service Connection with an Agent

| | |
|---|---|
| **Function** | `rollback` |
| **Ontology** | `FIPA-VPN-Provisioning` |
| **Supported by** | NMSWA |
| **Description** | The execution of this function has the effect of rolling back a service. |
| **Domain** | `service-connection` |
| **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 |

### 5.2.7 Termination of a Service Connection with an Agent

| | |
|---|---|
| **Function** | `terminate` |
| **Ontology** | `FIPA-VPN-Provisioning` |
| **Supported by** | NPA and NMSWA |
| **Description** | The execution of this function has the effect of terminating a service. |
| **Domain** | `service-connection` |
| **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 |

### 5.2.8 Get Additional Requirements

| | |
|---|---|
| **Function** | `get-requirements` |
| **Ontology** | `FIPA-VPN-Provisioning` |
| **Supported by** | User Agent |
| **Description** | The execution of this function has the effect of requesting additional user requirements and preferences from the user agent. |
| **Domain** | `service-description` |
| **Range** | `service-description` |
| **Arity** | 1 |

# 6 References

[FIPA00029] FIPA Contract Net Interaction Protocol Specification. Foundation for Intelligent Physical Agents, 2000. http://www.fipa.org/specs/fipa00029/

[FIPA00030] FIPA Iterated Contract Net Interaction Protocol Specification. Foundation for Intelligent Physical Agents, 2000. http://www.fipa.org/specs/fipa00030/

[FIPA00067] FIPA Agent Message Transport Service Specification. Foundation for Intelligent Physical Agents, 2000. http://www.fipa.org/specs/fipa00067/

[FIPA00070] FIPA ACL Message Representation in String Specification. Foundation for Intelligent Physical Agents, 2000. http://www.fipa.org/specs/fipa00070/

[FIPA00079] FIPA Agent Software Integration Specification. Foundation for Intelligent Physical Agents, 2000. http://www.fipa.org/specs/fipa00079/