FORM

IST-1999-10357

Engineering a Co-operative Inter-Enterprise Management Framework Supporting Dynamic Federated Organisations Management

Document Number:	IST-1999-10357/LMD/WP4/0522_AnnexB
Title of Deliverable:	Deliverable 11 Final Inter-Enterprise Management System Model **Annex B, F-VPN System Model**
Deliverable Type: (P/R/L/I)*	P
Nature of the Deliverable: (P/R/S/T/O)**	R
Contractual Date of Delivery to the CEC:	28 February 2002
Actual Date of Delivery to the CEC:	28 February 2002

Workpackage responsible for the Deliverable:	WP4
Editor:	Henrik Røn (LMD)
Contributor(s):	ATOS, DLT, LMD
Reviewer(s):	Stefan Penter (DLT), Vincent Wade (TCD)

ABSTRACT

This Annex to FORM Deliverable 11 presents the final inter-enterprise management system model for the Fulfilment-VPN Provider.

KEYWORDS

IP VPN, Security, QoS, System Model, Business Model, Analysis Model, Building Block, Contract specification

* Type: P:Public, R-Restricted, L-Limited, I-Internal

** Nature: P-Prototype, R-Report, S-Specification, T-Tool, O-Other

IST-1999-10357

FORM

Deliverable D11

Final Inter-Enterprise Management System Model

Annex B, F-VPN System Model

Editor : **Henrik Røn**

Status – Version : Final
Date : **28 February 2002 (of document release)**
Distribution : Public
Code : IST-1999-10357/LMD/WP4/0522_AnnexB

The FORM Consortium consists of:

Atos Origin Intégration (France) – *Project Coordinator*
Broadcom Eireann Research Ltd. (Ireland)
DELTA Danish Electronics, Light & Acoustics (Denmark)
Fraunhofer FOKUS (Germany)
LM Ericsson A/S (Denmark)
TDC Tele Danmark A/S (Denmark)
Trinity College Dublin (Ireland)
UH Communications A/S (Denmark)
University College London (UK)
Waterford Institute of Technology (Ireland)
KPN Research (The Netherlands)

Table of Contents

1 Introduction

Fulfilment-VPN, hereafter referred to as VPN, is the part of the Fulfilment process, which deals with management of secure connections with guaranteed Quality of Service (QoS).

This document presents the final system model done in FORM within the VPN Business Process Area. It demonstrates how the FORM methodology is applied to the problem of providing a VPN service. The QoS part of this process is described in [FORM D11, Annex C]. It should be noted that only key functionality is handled. The system models can be regarded as the result of the first system development iteration.

The FORM methodology "Building Block Development Guideline" [FORM D12] is applied to the VPN Domain in the following way:

FORM D12 Building Block Development Guideline – Workflows:	FORM D11 – FORM methodology applied in Sections:
1.Perform Business Modelling Workflow	Section 2 Business Model 2.1 Business Use Case Model 2.2 Business Object Model
2. Define Reference Architecture Workflow	2.3 Reference Architecture
3. Define Requirements Analysis Workflow	Section 3 System Model 3.1 Use case Model
4. Develop Analysis Models Workflow	3.2 Analysis Model
5. Re-organise Analysis Models Workflow	3.3 Re-organise Analysis Model and Group to Building Blocks 3.4 Building Block Specification

Table 1-1 Mapping between FORM Methodology and VPN System Models

The Fulfilment VPN Business Model in Section 2 sets the context for the system model by presenting the business use cases and business object model. The reference architecture is also presented.

The VPNS Provider System Model is presented in Section 3. System modeling involves the identification of the functionality necessary to support the system and the design of the software components necessary to provide that functionality.

First use cases and actors are identified and explained in Section 3.1. Then analysis objects that implement the use cases are identified and the interactions documented in Section 3.2. Having identified the analysis object the next step is to group these object into Building Blocks and specify their contracts, this is shown in Section 3.3 and 3.4. The complete set of contract specifications can be found in the on-line contract catalogue at the FORM website [FORM Contracts].

2 Fulfilment VPN Business Model

There is a growing need for geographically dispersed organisations to connect in an efficient, cost-effective manner, where connections are secure and have guaranteed quality of service (QoS) properties. This need has created a new link in the e-business value chain, namely the Virtual Private Network (VPN) Service Provider. VPN is the main enabler in the new B2B environment, allowing users to connect to the corporate network from wherever, whenever needed. Thus, users can benefit of the public framework of the Internet to constitute a VPN as an economic viable alternative to leased line networks. The main advantage of VPN solutions, compared to leased lines, is flexibility. Customer needs will be more and more focused on dynamic cooperation.

In the FORM context, a VPN is a group of two or more computer systems, which typically are part of a private network with limited public-network access. VPN offers enterprise-scale connectivity deployed on a shared public infrastructure, while enjoying the same policies as a private or leased network. Such policies include security, guaranteed QoS, prioritisation, reliability and end-to-end management.

Also, a VPN is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunnelling protocols and security procedures. A VPN can be contrasted with a system of owned or leased lines that can only be used by one company. The business case of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one. Companies today are looking at using a VPN for both Extranets and wide-area Intranets.

Based on the above arguments it seems obvious that providing VPN services based on Internet infrastructure is a key market area within the e-Business segment. Such VPN services are called IP VPN services and can be functionally separated into at least three categories:

- Intranet VPN: Between a corporation and its branch offices.
- Remote access VPN: Between a corporation and its remote or travelling employees.
- Extranet VPN: Between a corporation and its business associations (partners, customers, suppliers or investors for instance).

The IP VPN services developed within FORM have been based on definition and study of Business Cases, one such case study (the MRITech scenario) is presented in [FORM WP19].

In the following part a summary of requirements is presented.

The customer of the VPN Service Provider (VPN SP) can be an organisation as well as an Application Service Provider (ASP), both aiming at outsourcing management of communication links to a third party called Inter-Enterprise Service Provider (IESP) in FORM. In the following the customer of the VPN SP is called VPNS Customer. The following requirements formed the basis for definition of FORM IP VPN service and are derived from two main actors: VPNS Customer and VPN SP.

First the main VPNS customer requirements:

- **Dynamic service activation**. A B2B context requires a high level of flexibility regarding set up and activation of communication links. Today it is crucial to provide services that can be adapted on the fly based on specific needs. Moreover, such needs change frequently based on business context and the applications used.
- **Guaranteed QoS**. A requirement from the B2B market segment is the ability to provide connections with guaranteed end-to-end QoS. Moreover, different kinds of applications will be used and therefore request different levels of QoS.

- **Specific level of security**. In a B2B context security is a main enabler. Use of intranets and extranets requires a high level of trust between the participants and therefore the VPN must ensure secure connections. In addition, different levels of security need to be provided to the and it must be possible to select the level of security on the fly based on the business context.
- **Outsourcing**. In the business model defined by FORM, a third party provides the VPN service. This takes into account the fact that more and more organisations want to focus on their core business and therefore prefer to outsource functionality such as communication links management.

Then the main requirements defined by the VPN Service Provider:

- **Automatic mapping from requirements to network configuration**. Enforcement and dynamic service activation based on input requires transformation of such input into a specific network configuration as well as enforcement of such a configuration at network level.
- **Possibility to map business requirement to different tunnelling mechanisms**. IP VPN provisioning can be based on various IP tunnelling mechanisms IPSec, L2TP, MPLS, etc. The VPN SP implements the VPN service based on one or more tunnelling mechanism. Therefore the IP VPN service must be able to handle multiple tunnelling mechanisms. This will allow the VPN service to adapt to the changing context of the Network Provider.
- **Provision of guaranteed QoS in combination with security**. IP tunnelling mechanisms are in principle dedicated to either QoS or security. Possibility to mix different tunnelling mechanisms allows accumulating benefits from each.
- **Guaranteed QoS over multiple ISPs**. As each ISP may use different types of network equipment, which may support different QoS mechanisms, the VPN SP must provide functionality to provide QoS across multiple ISPs with heterogeneous networks.
- **Outsourcing CPE management for set up of tunnels**. Again based on the fact that more and more organisations want to focus on their core business and therefore prefer to outsource functionality such as CPE management.
- **Customisation of the VPN service**. The service needs to be adaptable in order to accommodate changes in the market as in the network technology.
- **Full operation of the VPN service from an administrative console**.

All these requirements, plus requirements defined in [FORM D10], have been used for defining FORM IP VPN service solution. Only fulfilment processes for the VPN service has been developed within FORM. The FORM partners developing the IP VPN service (Atos Origin, Broadcom, DELTA, LM Ericsson) have chosen to use existing standards. The main standards and drafts deemed relevant for designing the VPN service are:

- [M.3108.1], [M.3108.3], [M3208.1] and [M.3208.3], as defined by ITU-T, which provide interfaces and information models for supporting operations between VPN customer and VPN SP.
- The IPSec policy model drafts [IPSec Configuration] and [IPSec Policy], as defined by IETF IP Security Policy Working Group, which bases configuration of IPSec tunnels on policies.
- Internet 2 Qbone [Internet2 QBone] for next-generation end-to-end QoS over multiple ISPs.

Other standards or draft standards have been minor influences during the design of the IP VPN service. But even though IP VPN is considered a major enabling service for B2B, specific standards supporting IP VPN are not mature and stable. This is described in more detail in [FORM WP19].

The rest of this annex provides reference models, which are the result of analysis and design of the IP VPN service in adherence to the FORM development methodology.

2.1 Business Use case Model

The context of the VPN system model is described in the main document of D11 and is shortly refrained in the business use case below. A Business Use case is the RUP equivalent of a business process description.

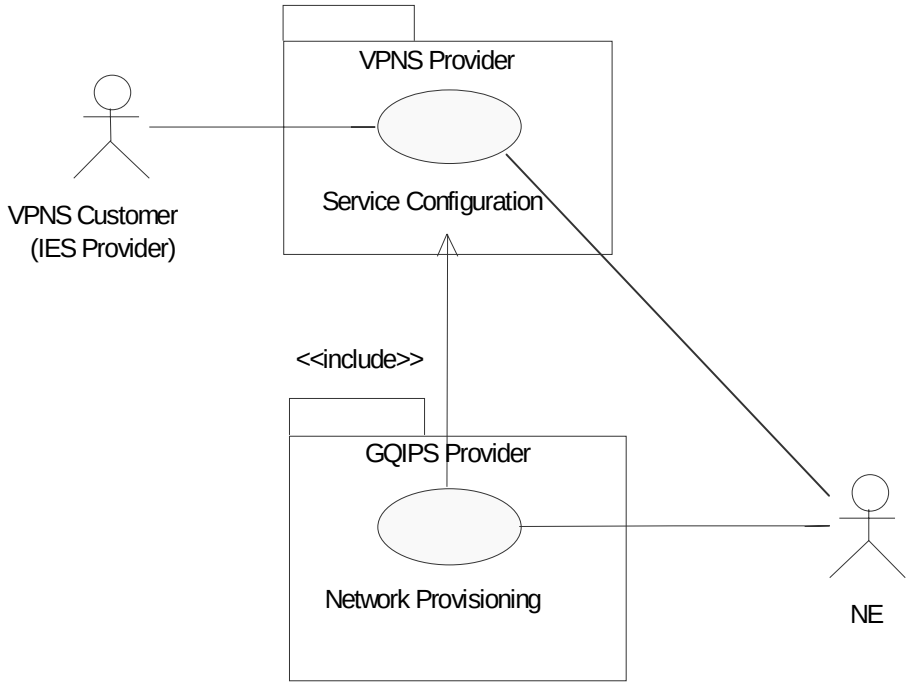

Figure 2-1 Business Use case diagram for VPN

Business Use case description for **VPN Service Configuration:**

1. The IES order handling (this could be replaced by any client using VPN Service) has passed on the order to VPN service configuration.
2. First the logical end-to-end path that the new service will run is determined.
3. Service configuration determines which device manager is responsible for the edge router and request that provisioning to be done by that particular device manager, e.g. Guaranteed QoS IP Service (GQIPS). Bandwidth reservation between VPN SP and GQIPS is based on a negotiation process, where GQIPS can accept, refuse or propose new numbers for the bandwidth. It is then up to the VPNSP to accept or not.
4. The VPNSP in the FORM project also provisions IPSec Tunnels, which assures the security between Customer Premise Equipment (CPE).
5. After the VPN service has been provisioned and activated VPN service configuration informs IES Order handling that the service has been provisioned and is now active.

Business Use case description for **Network Provisioning (GQIPS):**

1. The physical provisioning now takes place in the GQIPS
2. The provisioning process completes

Later in this document the business use cases are detailed by use cases excluding the GQIPS, which is described in Annex C.

2.2 Business Object Model

The business objects are responsible for carrying out the process described in the business use case.

Business Worker	Description
VPN Service	The purpose of the VPN Service (VPNS) is three-fold: (a) Maintaining an abstract virtual topology, which represents the participants in the VPN as access groups and access points, (b) to map from this virtual topology to concrete types of network, (c) establish the actual VPN connections using the IPSec Service and GQIPS.
IPSec Service	The IPSec service is responsible assuring the security between CPE

Table 2-1 VPN Business workers

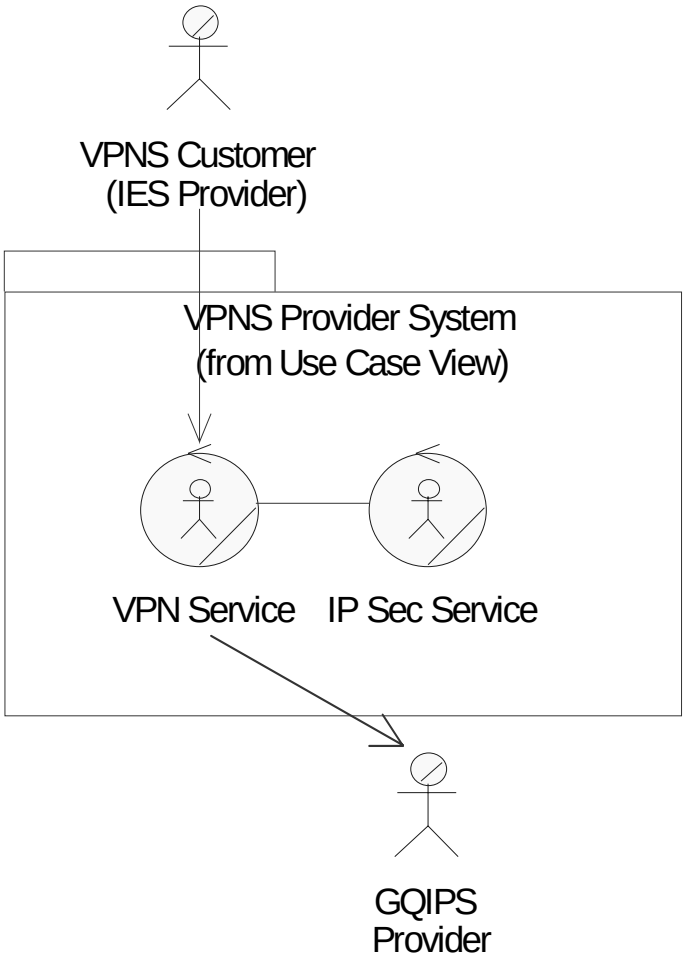

Figure 2-2 Business Object Model for VPN

The next section explains how the business workers fit into the reference architecture developed within FORM. See main D11 document, section 4.3 for an explanation of how the reference architecture has evolved.

2.3 Reference Architecture

The Figure below shows the part of the FORM reference architecture that is related to the Fulfillment-VPN business process.

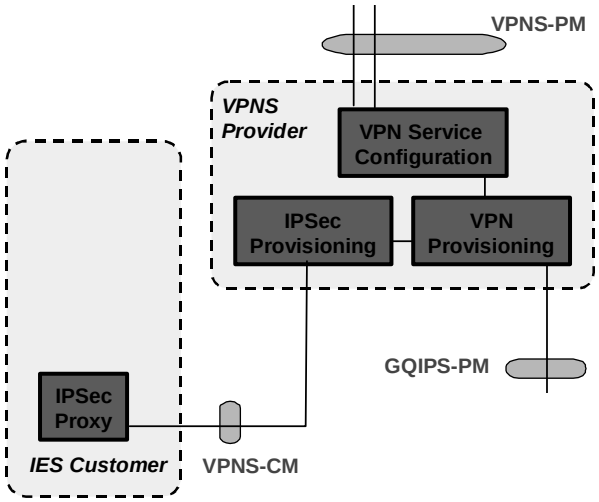

Figure 2-3 VPN subsystem within the Reference Architecture

The Figure above contains the initial VPN system reference architecture, the system boundary definitions of the roles relevant to the VPN subsystem and a decomposition of the subsystems relevant to the VPN into subsystems.

The VPN architecture contains two main reference points: VPNS-PM and VPNS-CM. They serve two distinct purposes:

- **VPNS-PM**. This reference point provides the functionality for managing the virtual topology, i.e. creating, modifying and deleting entities in the virtual topology and for creating, modifying and deleting the VPN connections in the virtual topology.
- **VPNS-CM**. Used by the IPSec Provisioning Manager for setting up IPSec tunnels on CPE.
- **GQIPS-PM**. Used for all QoS related tasks bandwidth reservation, connections activation, etc. This reference point and the models relating to it are described in Annex C and therefore the GQIPS is treated as an actor in this document.

In the next section it will be explained how the subsystems in the reference architecture are designed based on further analysis of the business process using system use cases.

3 VPNS Provider System Model

According to the business models and the reference architecture we split the VPN processes between two organisations, the VPN SP and the GQIPS Provider System (GQIPSPS). The use case model will reflect this.

3.1 Use case Model

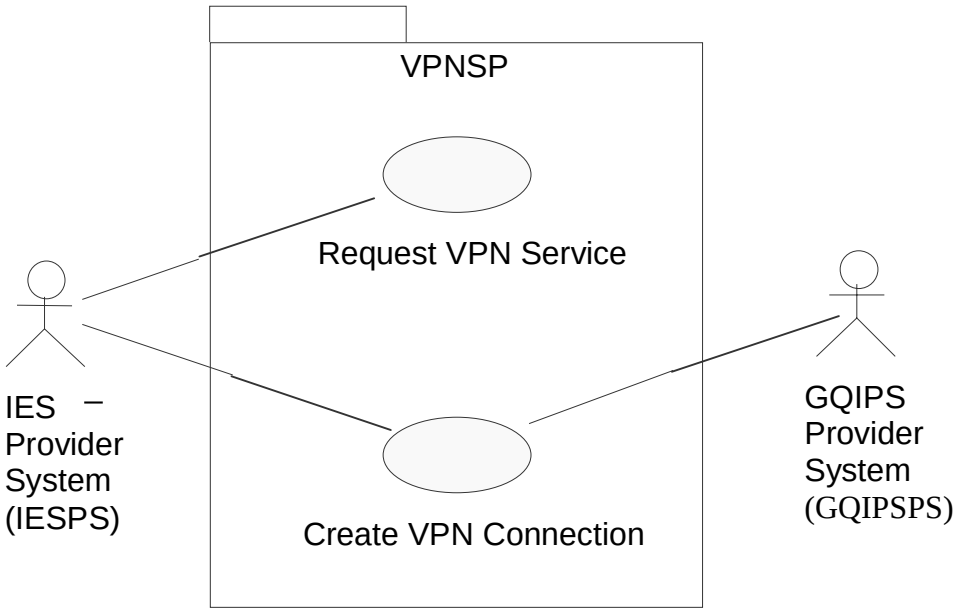

Figure 3-1 Use case diagram for the VPN Provider System

Actor Name	Role Taken
IES Provider system	The individual or organisation responsible for managing the IESP system and specifying the policies to be implemented by it.
GQIPS Provider system	Represents the underlying software and hardware that provide the IP connectivity between the various parties.

Table 3-1 VPN Actors

These actors participate in two main use cases “Request VPN Service” and “Create VPN Connection”, which are described in schematic form below.

Use case Name	Request VPN Service
Summary	The use case demonstrates how the VPNS Provider System (VPNSPS) creates a service instance for the VPNS Customer, i.e. the IESPS
Actors	IESPS and GQIPSPS
Pre-Conditions	The relationship between the IESPS and VPNSPS exists
Begins When	When an order (request VPN service) has arrived from the IESPS
Steps	The IESPS has passed on the order (request VPN service) with the parameters (Customer Contact, Service Class List, Alias Name, Access Points) to VPNSPS. The VPNSPS creates a service instance for the VPNS Customer. Then the logical end-to-end path between Access Points, "the virtual network topology" that the new service will run is determined.
Ends when	The VPN service has been created.
Post-Conditions	A virtual topology has been created inside the VPN system and the system is in a stable state and ready to receive new input.
Exceptions	An exception is raised, which must be caught by the IESPS and handled according to the nature of the exception (Invalid input, etc.)
Traceability	Business process: VPN Service Configuration

Table 3-2 Use case description of "Request VPN Service"

Use case Name	Create VPN Connection
Summary	The use case demonstrates how the VPNS Provider System fulfils the VPN order for the VPNS Customer by provisioning and activating a VPN connection
Actors	IESPS and GQIPSPS
Pre-Conditions	The relationship between the IESPS and VPNSPS exists and the service instance for the VPNS Customer has been created.
Begins When	When the VPN order (Create VPN Connection) has arrived from the IESPS
Steps	The IESPS requests the VPNSPS to create a VPN connection. The request contains parameters (Customer Contact, Alias Name, VPN_ID, Connection). The VPNSPS sends a reservation request with a list of RAR (Resource Allocation Requests) to the GQIPSPS. Further the VPNSPS provisions IPSecs, which assures the security between CPEs. After the VPN connection has been activated, VPN Service Configuration informs IESPS of the activation.
Ends when	The VPN service is activated and completion status passed back to the IESPS
Post-Conditions	Connection has been added to the virtual topology, actual connection has been created at the network level, the system is in a stable state ready to receive input.
Exceptions	An exception is raised, which must be caught by the IESPS and handled according to the nature of the exception (Invalid input, network failure, etc.)
Traceability	Business process: VPN Service Configuration

Table 3-3 Use case description of "Create VPN Connection"

3.2 Analysis Model

In this part we identify the analysis objects that will perform the steps on the use cases “Request VPN Service” and “Create VPN Connection”. The class relations are outlined in the following diagram.

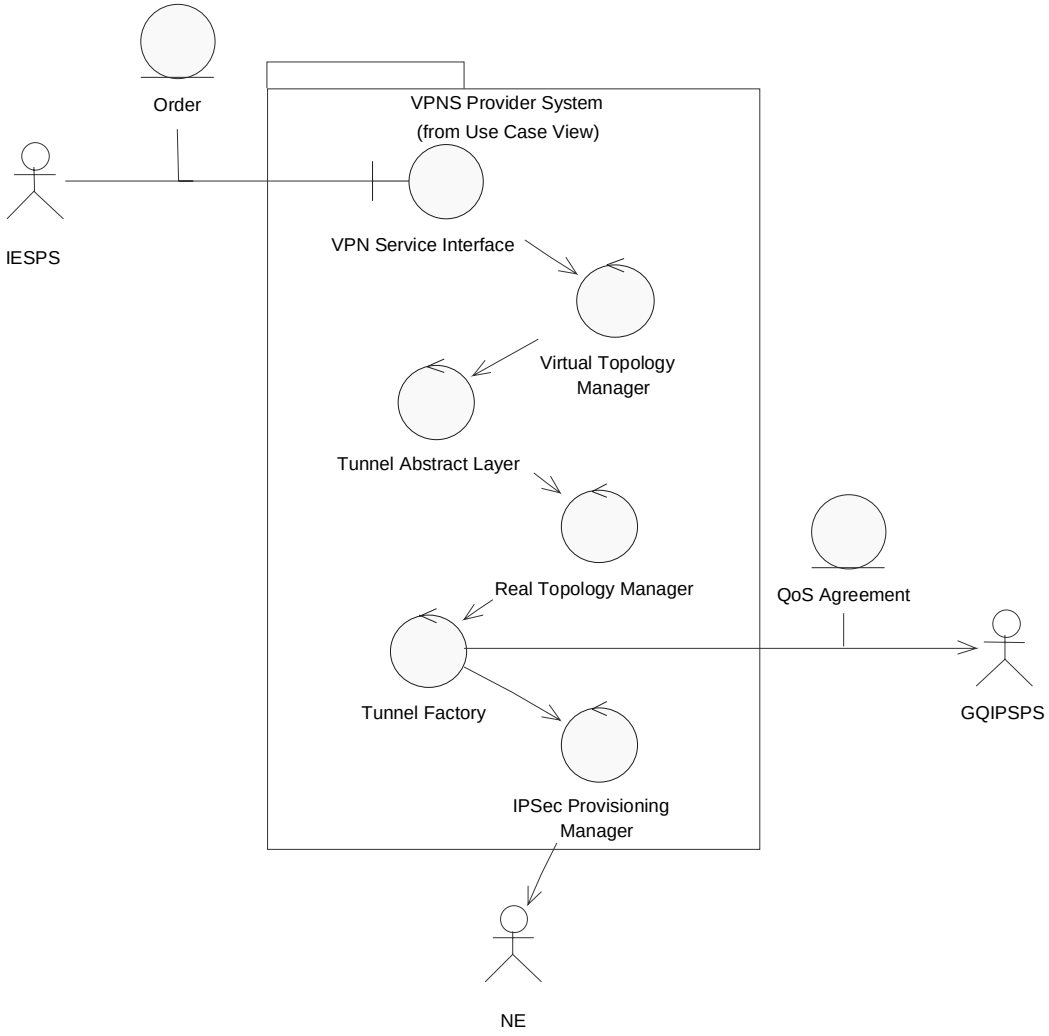

Figure 3-2 Analysis objects implementing use cases for VPN Service Configuration

The boundary, entity and control object from the figure above are described below.

3.2.1 Boundary Objects

Boundary Objects	Responsibility
VPN Service Interface	This object provides the interface of the VPNSPS towards the IESPS

Table 3-4 Boundary Objects

3.2.2 Entity Objects

Entity Objects	Responsibility
Order	The order object contains the data that the IESPS sends to the VPNSPS to initiate the use case "Request VPN service"
QoS Agreement	The GQIPSPS uses a Resource Allocation Request (RAR) object during negotiation for QoS allocation. Once the negotiation has been completed a RAR is return to the VPNSPS.

Table 3-5 Entity Objects

3.2.3 Control Objects

Control Objects	Responsibility
Virtual Topology Manager	Virtual Topology Manager: Handles the entities of the virtual topology, including VPN Service, SAP, SAG, VPN Connection.
Tunnel Abstract layer	Handles tunnel management and allows creation of the link mapping from a virtual topology to real network entities.
Real topology manager	Handles real network entities, mainly border nodes, thus allowing configuration of VPN links.
Tunnel factory	Allows creation of tunnels based on real topology information. The Tunnel factory can request creation of IPSec tunnels to IPSec Provisioning Manager as well as request for bandwidth reservation to GQIPSPS.
IPSec Provisioning Manager	The IPSec-Provisioning Manager object provides management services related to the configuration of IPSec tunnels. The object will control and manipulate IPSec tunnels through the use of IETF IPSec Provisioning Policies.

Table 3-6 Control Objects

The analysis object form an abstract system model where each object has a certain responsibility to carry out part of the use case. In the next section these abstract objects are grouped in Building Blocks and thus each Building Block has responsibility for several steps of the use case.

3.3 Re-organise Analysis Model and Group to Building Blocks

The grouping presented in this chapter is just one way of designing the system. The grouping chosen was influenced as much by design and architecture as by the fact that the work of developing the Building Blocks was divided upon partners, which were distributed geographically and parts of different organisations.

Our basic architectural style was a layered model. We grouped the two objects “VPN Service Interface” and “Virtual Topology Manager” into a “VPN-Service Configuration” Building Block responsible for providing the external interface to the VPN system, with functionality for virtual topology and high-level workflows for VPN and Connection management. The “Tunnel Abstract Layer”, “Real Topology Manager” and “Tunnel Factory” objects were grouped into a “VPN-Provisioning” Building Block, which deals with mapping from the high-level concepts to concepts closer to the network, and finally an “IPSec-Provisioning” Building Block for the IPSec Provisioning Manager, which manages the concrete IPSec tunnels as seen from within the VPN system. All these are also in the reference architecture in Figure 2-1 within the VPNS Provider domain. Furthermore another component is designed, the “IPSec Proxy”, which is responsible for enforcing the IPSec tunnel configuration on the CPE. This component plays the role of an IPSec Policy enabled CPE.

All these Building Blocks and their interactions are shown in the figure below. As the “IPSec Proxy” component is in the “IESP Customer” domain it is not shown in the figure below, but it is still in the reference architecture.

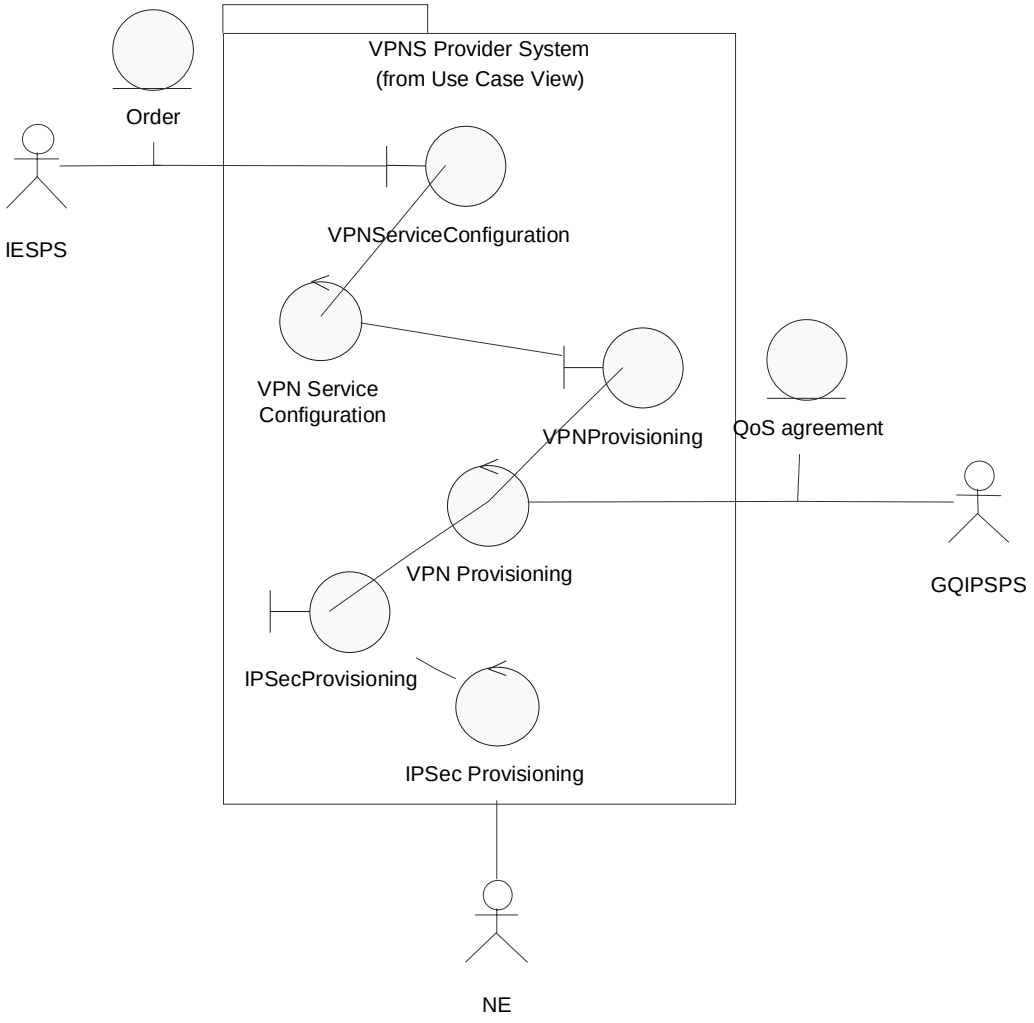

Figure 3-3 Collaboration diagram – Building Blocks and Building Block Contracts

The following sequence diagram shows more details about the relations between the building blocks and the actors.

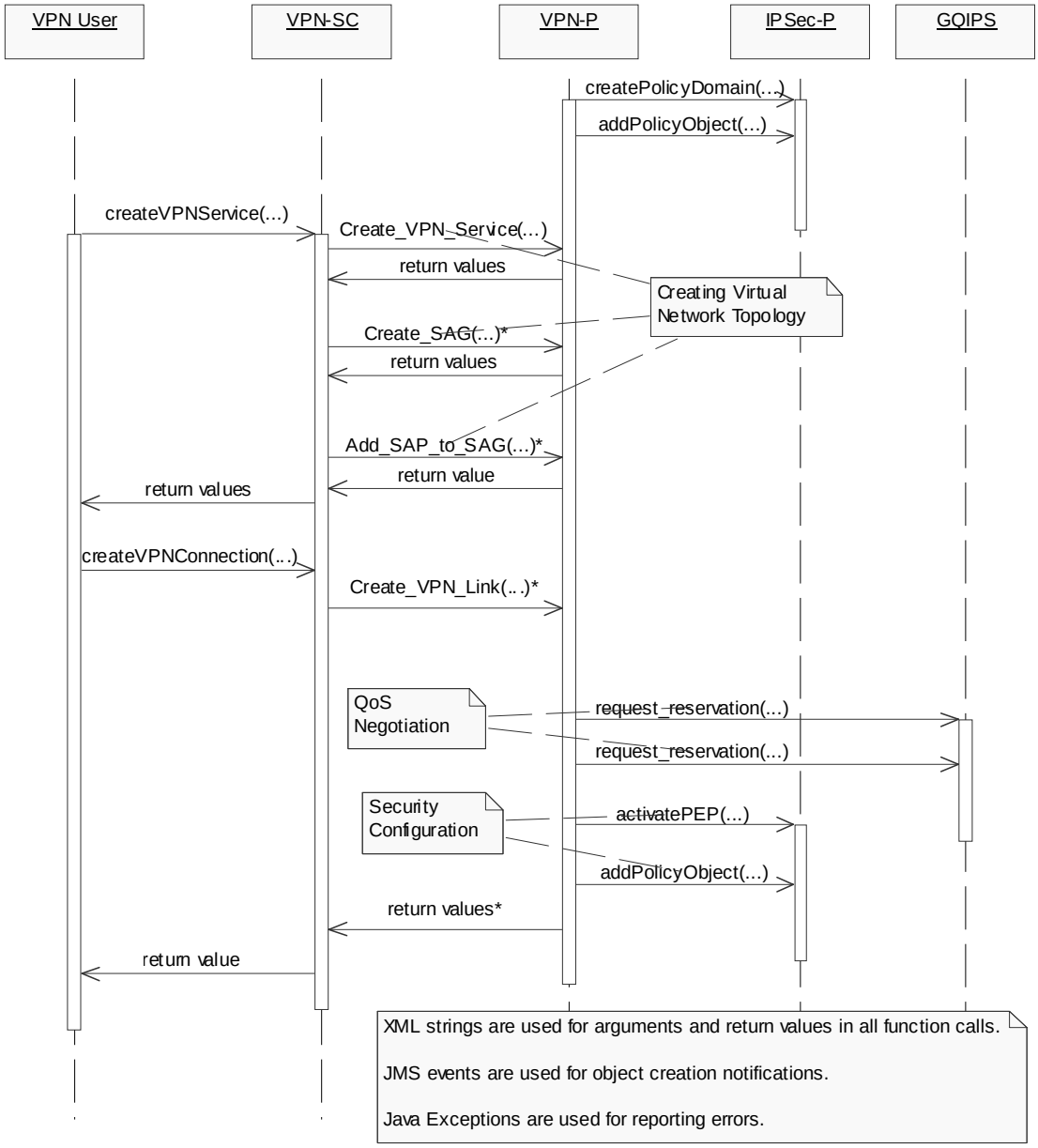

Figure 3-4 Interaction diagram for" VPN Service Configuration" showing the use of BB

3.4 BB Contract specification

Four contracts have been specified for the Fulfilment-VPN system based on the XML Schema described in Annex E. These can be found in the on-line contract catalogue at the FORM website [FORM Contracts].

4 Conclusion

The purpose of this annex has been to demonstrate the application of the FORM methodology on the Fulfilment-VPN system. It shows how the Business Object Model can be broken into Use Case Models and how these can be used to identify analysis object before finally mapping to the building blocks for implementation. The analysis presented does not cover all use cases needed for dynamic provisioning of secure, guaranteed QoS IP VPN.

5 References

[FORM Contracts] Index to the Contract catalogue:

http://www.cs.ucl.ac.uk/research/form/models/ContractCatalogue/

[FORM D10] Quinn, Niamh, "D10: Validation of Inter-Enterprise Management Framework", IST-1999-10357/BRI/WP5/02xx, due February 2002.

[FORM D12] Wade, Vincent, "D12: Guidelines for Co-operative Inter-Enterprise Management", IST-1999-1057/TCD/WP3/012, February 2002.

[FORM WEB] The FORM project homepage http://www.ist-form.org

[FORM WP19] "Providing dynamic VPN services for B2B", available from [FORM Web] under "Results" → "White Papers"

[Internet2 QBone] Various standards for QoS according to QBone are available at http://qbone.internet2.edu/

[IPSec Configuration] IETF IP Security Policy WG: "IPsec Configuration Policy Model", Draft v/2, draft-ietf-ipsp-config-policy-model-02.txt

[IPSec Policy] IETF IP Security Policy WG: "IPSec Policy Information Base", Draft v/2, draft-ietf-ipsp-ipsecpib-02.txt

[M.3108.1] ITU-T Recommendation M.3108.1: "Information Model for Management of Leased Circuit and Reconfigurable Services"

[M.3108.3] ITU-T Draft M.3108.3: "Information Model for Management of Virtual Private Network Service"

[M.3208.1] ITU-T Recommendation M.3208.1: "TMN Management Services for Dedicated and Reconfigurable Circuits Network: Leased Circuit Services"

[M.3208.3] ITU-T Draft M.3208.3: "TMN Management Services for Dedicated and Reconfigurable Circuits Network: Virtual Private Network Service"

[W3C XHTML] "XHTML™ 1.1 – Module-based XHTML", W3C Recommendation 31 May 2001, http://www.w3.org/TR/xhtml11/