FORM

IST-1999-10357

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

Document Number:	IST-1999-10357/ATOS/WP6/3010
Title of Document:	White Paper: Providing dynamic VPN service for B2B
Restrictions: (P/R/L/I)*	R
Nature of the Document: (P/R/S/T/O)**	P

Workpackage responsible for the Deliverable: WP6

Editor: Hervé Karp (Atos Origin)

Contributor(s): Stefan Penter (DELTA), Henrik Ron (LM Ericsson)

Reviewer(s):

ABSTRACT

The purpose of this white paper is to present the work done in the VPN Working Group of the FORM project. It presents the role of advanced IP VPN in B2B with a scenario and the solution implemented by the partners.

KEYWORDS

IP VPN, IPSec, Service Configuration, Provisioning, GQIPS, Service Class, Policy.

See http://www.ist-form.org for further details

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

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

IST-1999-10357

FORM

White Paper

Providing dynamic VPN service for B2B

Editor :	Hervé Karp (Atos Origin)
Status – Version :	First Version
Date :	18/03/2002
Distribution :	Public
Code :	IST-1999-10357/ATOS/WP6/3010

The FORM Consortium consists of:

Atos Origin Intégration (France) – *Project Coordinator*

Broadcom Eireann Research Ltd. (Ireland)

DELTA Danish, Electronics, Light & Acoustics (Denmark)

GMD 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

This paper will present you some results from FORM a European R&D project partially funded by the European Commission. You can find more details about FORM from the web site: http://www.ist-form.org/ .

The focus of this project is the definition and validation of an Open Development Framework (ODF) supporting development of management systems dedicated to management of B2B services over QoS enabled IP networks. Therefore study of B2B services and e-Business value chain is one keystone in this project.

In the Business-to-Business value chain, providing "e" services means much more than building web-front interfaces with fancy features to end customers. An e-Business value chain can be defined as commerce conducted between businesses over an Intranet, Extranet or Internet (i.e. IP Networks). The rapid of growth in e-Business is enormous. While organisations in different countries move online at their own pace, their collective e-Commerce activities is estimated, by Forester Research Inc. to reach $6.8 trillion dollars, or 8.6% of the global sales of goods and services, in 2004 [Sand00].

A key aspect in successful e-Business operation is the optimisation of the e-Business value chains (i.e. management of business-2-business chains) [OConn00]. Thus a crucial element of successful e-Business operation is the ease and flexibility of *integrating and managing* inter business interaction. However, in ever increasing competitive markets, organisations are focusing on their own key market competencies and seeking *outsource managed solutions* for non-core competencies. Such e-Business requirements provide new opportunities and challenges for next generation Internet and Telecommunication service providers. To support e-Business across supply/value chain, these next generation Internet and Telecommunication providers must offer *dynamic, managed communication and inter-organisational application service managemen*t.

Thus, in much the same way as organisations have become reliant on third party managed connectivity services, e-Businesses are beginning to seek managed e-Business networks where the *e-Business value chain is managed and supported as an integrated service*. Providers of such e-Business management services must provide managed solutions across e-Business value chains (end to end management of B2B supply chains).

Current e-Business managed solutions, where available, tend to concentrate on only single aspects of the e-Business integration e.g. outsourced accounting management or traditional Virtual Private Network services. This is analogous to first generation telecommunication management systems that delivered stand-alone management applications for specific management concerns e.g. performance management, configuration management. However, the lessons learned from such ‘stove pipe’ management applications were that management function integration was vital to support increasing customer demands. However such integration was difficult if not impossible, if integration had not been considered from the outset. Thus, rather than developing piece-meal, isolated e-Business management applications, more functionally integrated solutions are required. Thus e-Business management services must be constructible rapidly and dynamically across different management functional areas.

In the FORM project we call an e-Business management provider the “***Inter Enterprise Service Provider***” (IESP). The services provided by an IESP are termed the “***Inter Enterprise Services***” (IES). Examples of IESs could include: dynamic, on-demand Virtual Private Network services; outsourced management of customer premises equipment, communications services and inter-organisation application services. The functional areas for this management would include Quality of Service monitoring and management, security management, accounting management, etc.

This paper focuses on one fundamental key service to be provided by an IESP, i.e. a dynamic IP VPN service. In the FORM project such service has been developed by some partners of the FORM project: *Atos Origin, LM Ericsson, DELTA and Broadcom.*

Today, the major part of companies is multi-locations so that, at each new merger, communications and exchanges between different subsidiaries are more and more difficult. Network managers must continually find ways to connect geographically dispersed work groups in an efficient, cost-effective manner. On top of that, the number of partnerships and relations between customers and suppliers is constantly growing. To make communications and exchanges always possible and secure the use of telephone or fax is not enough anymore. It seems VPN is a main enabler in the B2B environment, allowing users to connect to the corporate network whenever, wherever, or however they require. Thus, users can benefit of the Internet public framework to constitute a Virtual Private Network as an economic alternative to the leased line network. One main advantage of VPN solutions, compared to leased lines, is the flexibility. The customers needs will be more and more focused on possibility for dynamic cooperation.

In common usage a Virtual Private Network is a group of two or more computer systems, typically connected to a private network with limited public-network access. VPNs offer enterprise-scale connectivity deployed on a shared infrastructure with the same policies enjoyed in a private network. These 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 protocol and security procedures. A Virtual Private Network can be contrasted with a system of owned or leased lines that can only be used by one company. The idea 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. Phone companies have provided secure shared resources for voice messages. A VPN makes it possible to have the same secure sharing of public resources for data. Companies today are looking at using a VPN for both Extranets and wide-area Intranets.

From this point it seems obvious that providing such VPN services based on Internet infrastructure is a key market around e-Business. Such VPN services are now called IP VPN services and can be functionally separated in three categories:

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

In the today IP VPN market some strong requirements, regarding IP VPN service, from customers but also from Service Providers are not fulfil. These requirements have been integrated by FORM partners in the design of the FORM IP VPN service. Therefore, solution as well as concepts and principles used are quite innovative. Within this project we had the opportunity to validate a first prototype and to demonstrate these results to potential customers such as European Telecommunications Operators.

The approach to define our IP VPN service has been based on definition and study of Business Cases. This paper presents, in second section, one case study (MRITech scenario), which provides concrete vision of requirements. Then, in section three, the solution designed by the consortium is presented with specific highlight on main principles integrated to this design. The paper concludes with future work in the development of the FORM IP VPN service and highlights main benefits of such solution compared to today solution from the market.

2 MRITech Scenario

MRITech scenario defines a set of inter-enterprises collaboration activities. It illustrates some concrete requirements in a specific business environment. However, end user requirements extracted from this scenario are generic and could be applied to other virtual enterprise scenarios. FORM IP VPN solution integrates such requirements and provides therefore a very innovative solution as today VPN solutions on the market does not fulfil the whole requirements.

MRITech is a developer of medico equipment. Their main product is a Magnetic Resonance Image (MRI) scanner, which is an IP-enabled device. The IP enabling serves several purposes.

The producer can perform remote operation, service and maintenance. Doctors and experts can provide on-line assistance in patient diagnostics or specialised usage of the equipment. The scanner supports integration with electronic patient records, or other database-related facilities.

Rather than providing medical equipment to their customers, the IP enabling of the scanner allows MRITech to act as an Application Service Provider (ASP), providing the service of MRI imaging at the customer’s premises such as hospitals or clinics.

MRITech’s core competency lies in the area of MRI imaging techniques, but they do not have interest or expertise in some of the other aspects of the application service such as communication technology, management of communication links or management of data generated by the MRI scanner. This leads to a requirement for off-the-shelf components to be included in the MRI scanner providing communications functionality and management capabilities, as well as usage of third party service providers for connection management and database facilities. Connection management will be outsourced to an Inter-Enterprise Service Provider (IESP) and database facilities will be provided by a Data Base Service Provider.

The figure below shows the different actors of this business case as well as their relationships.

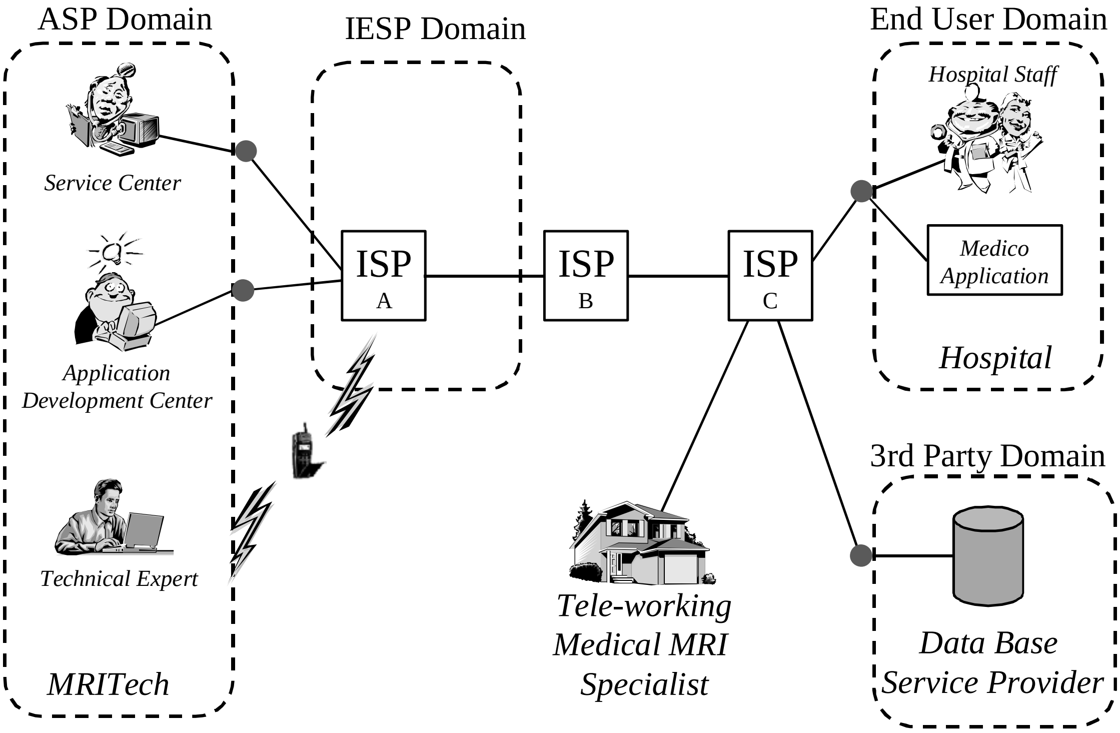

Figure 1: The MRITech scenario

The role of each actor of the MRITech scenario is presented below.

The Inter-Enterprise Service Provider (IESP) provides communication links based on an SLA (Service Level Agreement) defined with the MRITech Service Center.

Working with medical applications leads to a requirement for controlled reliability of the equipment, its operation and the facilities, including both communication and application level facilities, on which the application is based. Additionally a high level of security is required due to the confidential nature of the data generated by the application.

The number of players and the requirements of the connections between the players, vary according to the operation of the application. This leads to a requirement for dynamic establishment and configuration of both network and monitoring of the application layer connections between the players. The main characteristics of the connections are described below.

The Application Service Centre is the core part of MRITech, and is responsible for performing scheduled check-up or simple on-line service tasks of the Medico Application. Additionally the Medico Application issues alarms and trouble reports to the Application Service Centre in case of malfunctions. In the event of trouble the Application Service Centre can perform online service on the equipment to correct the problem, or acquire assistance from the Application Development Centre.

It is the MRITech that establish a Service Level Agreement (SLA) with the IESP for managing tunnelling, security and outsourcing. Following a service subscription by the end-customer (Hospital) the ASP has the required information for negotiating an SLA with the IESP.

The Application Development Centre, who is part of MRITech, is the organisation developing the IP-enabled Medico Application and has in-depth technical knowledge of the application. The Application Development Centre joins the VPN on request from the Service Centre, in order to provide assistance in trouble finding in case of application malfunction. Additionally the Application Development Centre is responsible for performing software upgrades of the Medico Application as new versions becomes available. Although the Application Development Centre is part of the ASP it may be located in a different geographical location than the Application Service Centre.

The Medical Expert, who is associated with MRITech, use audio/video services in order to provide on-line assistance or advice to hospital staff for specialised usage of the Medico Application. The Medical Expert is a mobile user, connecting to the Medico Application or hospital staff in case of emergency. The required VPN links between the Medical Expert and the Hospital are established by the IESP on the initiative of the ASP, following a request from the hospital.

The Hospital is the customer of the MRITech services. Through the subscription to the ASP, the hospital outsource the management of their corporate firewall or tunnelling gateway to the IESP, in order to allow management of the dynamic access to the hospital network and the Medico Application from various ASP sub-providers and application related 3rd party providers.

The Database Service Provider is a third party service provider responsible for storing and managing Medico Application output data for example as part of electronic patient records. Due to the confidential nature of patient data the VPN tunnels connecting the Database Service Provider and the Hospital has a strong requirement for a high level of security. The database service provider is expected to provide application level guarantees on the performance of its services.

Communication links requirement

The MRITech scenario involves a set of activities related to scanning operations as well as maintenance operations. In this part each interaction between actors of the MRITech scenarios are presented and specific communication links requirement are defined.

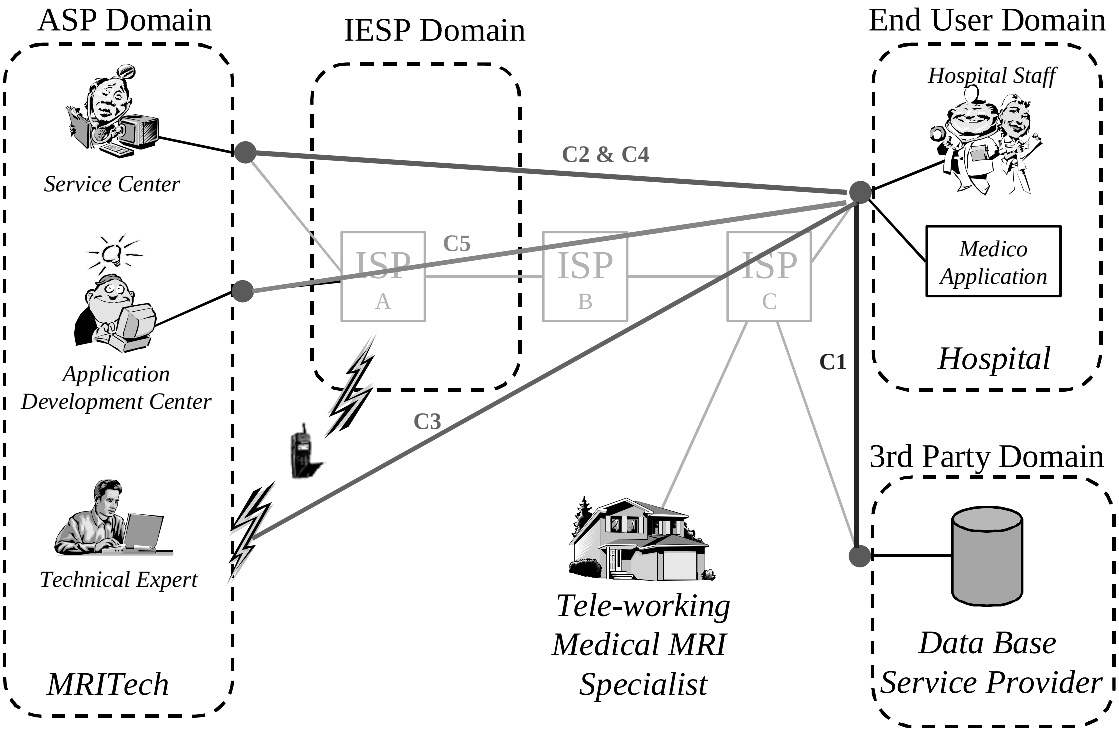

Figure 2: Communication Links in the MRITech scenario

C1. During scanning operation the MRI scanning application at hospital requires a VPN connection to the Database Service Provider for storing or retrieval of images or patient records. The database service provider is guarded by a firewall and the MRI Scanner at hospital is behind the hospital firewall. *Characteristics of the communication link (C1) are described in the table below.*

C2. During scanning operation, the MRI scanner requires a connection with the MRITech Service Centre for issuing alarms or trouble reports. *Characteristics of the communication link (C2) are described in the table below.*

C3. During operation, remote (dial-in) technical experts may participate in on-line operation of the equipment. The remote mobile medical expert is not guarded by a firewall. *Characteristics of the communication link (C3) are described in the table below.*

C4. During standard maintenance or upgrading of MRI scanning application, a connection is required between MRITech service centre and the MRI scanner at hospital, for download of software updates or inspection and tuning of service parameters. *Characteristics of the communication link (C4) are described in the table below.*

C5. During faultfinding, the MRI scanner requires a connection with MRITech Service Centre and MRITech Development Centre for support of debugging and consultancy/discussion between service personnel, technical experts and system developers. The development centre computers are guarded by a firewall. *Characteristics of the communication link (C5) are described in the table below.*

Communication Link	**Characteristics**
C1	- High bandwidth (lots of data being generated) - High security level (confidentiality of patient data) - Long lived connection
C2	- Low bandwidth (not much data for alarms or trouble reports) - Assured reliability of transmission (alarms should never be lost) - Low delay (alarms should be transferred immediately) - Long lived connection
C3	- High bandwidth (e.g. support of audio/video conferencing) - Highly reliable (actively working with a patient) - High security (confidentiality of patient data) - Quick establishment of connection - Short lived connection
C4	- Medium bandwidth - Standard reliability - Short lived connection

C5	- High bandwidth (e.g. support of audio/video conferencing, remote debugging, etc.) - Standard reliability - Quick establishment of connection - Multiple users on the same channel - Short lived connection

Table 1 Characteristics of the Communication Links

3 System Model

This section presents IP VPN Service Provisioning solution which is one result of the FORM project. Development of Building Blocks compounding this solution is based on the FORM Open Development Framework (ODF) methodology guideline. More information on FORM ODF and accompanying methodology can be found in [formD9] and [formD12].

The organisation operating the VPN Service is called the VPN Service Provider (SP), which could correspond to the IESP as defined in the previous section. The customer of the VPN SP can be an organisation as well as an Application Service Provider (ASP). The following requirements formed the basis for definition of FORM IP VPN service and are derived from two main actors: VPN end-user and VPN SP.

First the main end-user 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 end-users with services that can be adapted on the fly based on specific end-user 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, end-users will use different kinds of applications 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 guarantee the security of the connections. In addition, different levels of security need to be provided to the end-user and it must be possible for the end-user 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 SP:

- **Automatic mapping from end-user requirements to network configuration**. Enforcement and dynamic service activation based on end-user 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 [formD10], have been used for defining FORM IP VPN solution. Only fulfilment processes for the VPN service have 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 Service Provider.
- The IPSec policy model [IETF IPSec Conf, IPSec Policy], as defined by IETF, 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 the conclusion is that even though IP VPN is considered a major enabling service for B2B, specific standards supporting IP VPN are not mature and stable.

The virtual topology is based on the following concepts from [M.3108.3]:

- **Tunnel (Connection)**. The tunnel is a point-to-point connection between two VPN users.
- **Service Access Point (SAP)**. One SAP describes the location of a VPN user. Connections are established between SAPs.
- **Service Access Group (SAG)**. The SAG is a geographical location, which can have one or more SAPs attached. SAGs are mainly used for grouping SAPs.

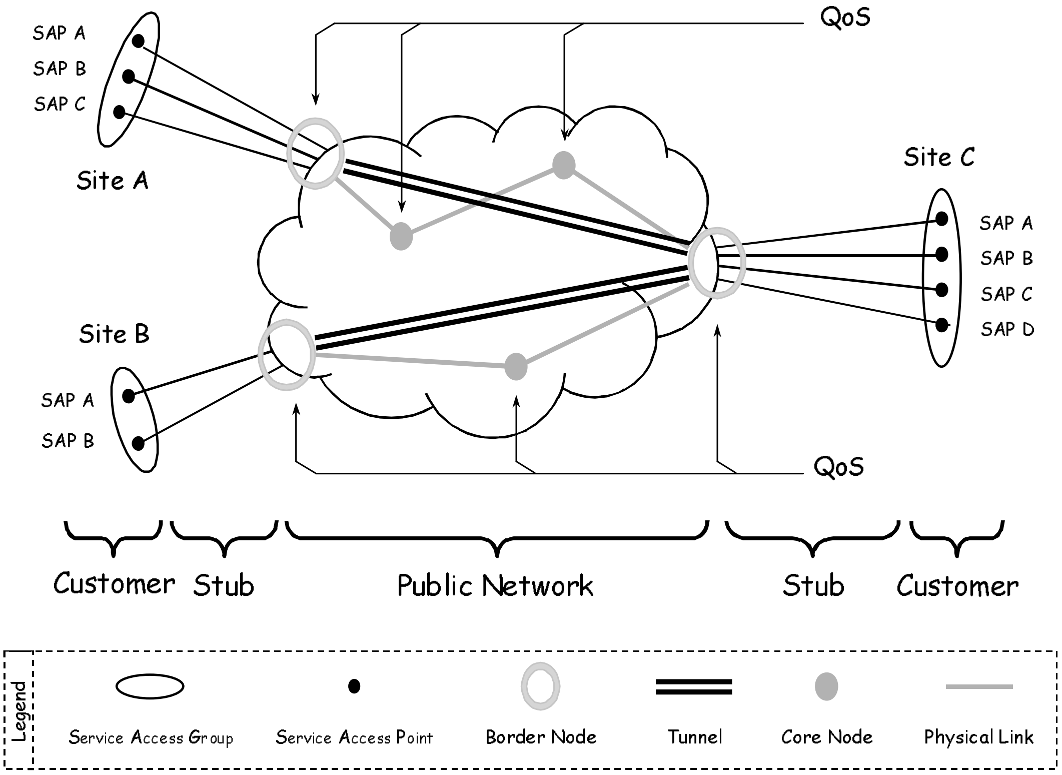

Figure 3: Virtual Topology of the VPN Service

These concepts are realized in a layered system as illustrated in the Figure below, where the top layer, VPN Service Configuration, is the only one accessible to the VPN user.

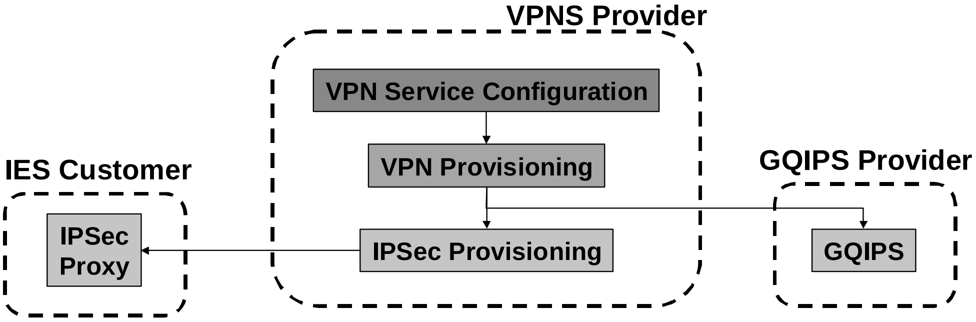

Figure 4: System division in layers

The higher layers are thus responsible for network technology independent tasks and processes and lower one goes in the layering, the more network technology related the tasks become. Figure 5 shows the analysis objects identified in FORM for VPN Provisioning.

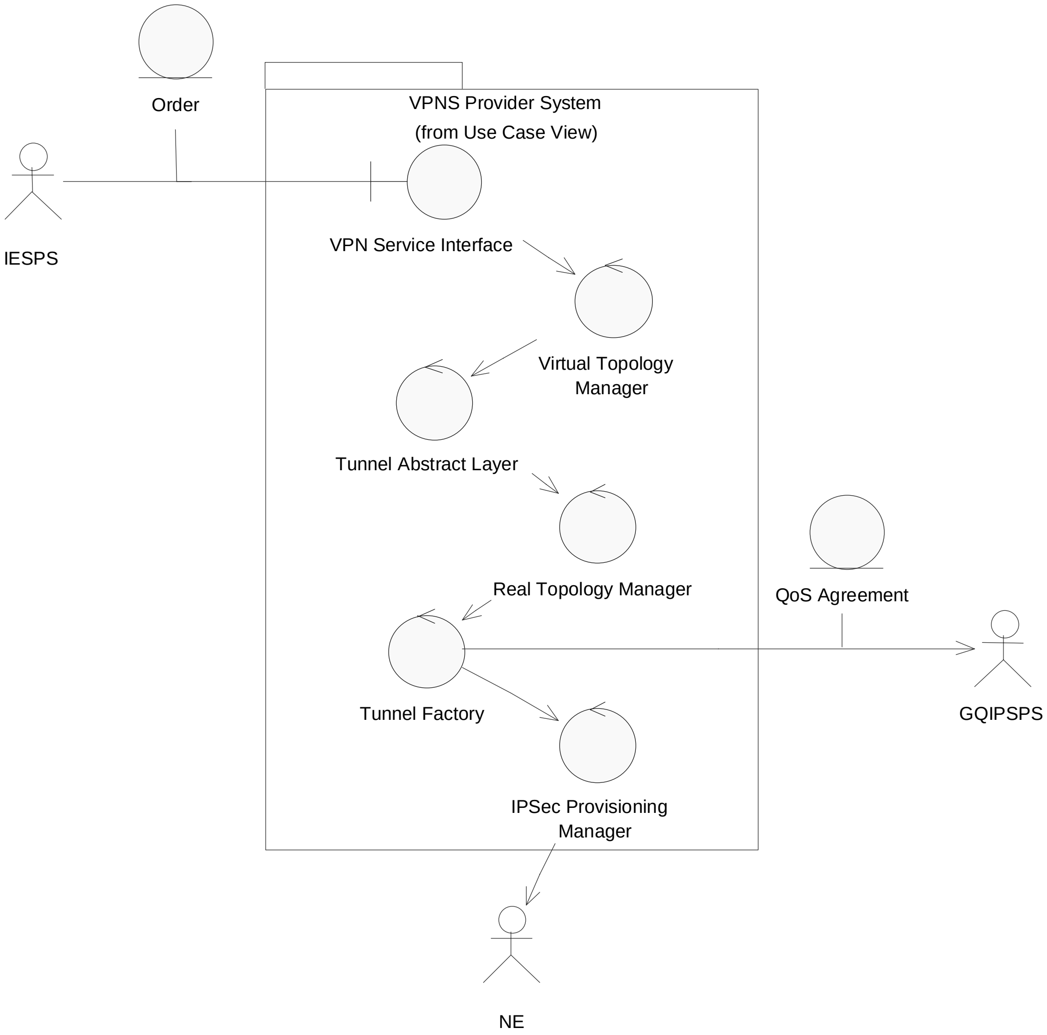

Figure 5: Analysis objects implementing use cases for VPN Service Configuration

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

Boundary Objects

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

Table 2 Boundary Objects

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 Entity Objects

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, which are the entities referred by the end user.
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 and transformation of end user requirement (defined through Service Classes). 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 4 Control Objects

The analysis objects are distributed onto the layers in the following way:

- **VPN Service Configuration**. Developed by L.M. Ericsson.
    - VPN service interface. The high-level management functions.
    - Virtual topology manager. The virtual topology manager, which maintains a totally technology independent topology.
- **VPN Provisioning**. Developed by Atos-Origin.
    - Tunnel abstract layer, which handles abstract view of tunnel, i.e. independent of underlying technologies.

  - Real topology manager, handles network topology entities useful for building VPN Links.
  - Tunnel factory, which request creation of tunnels at network level based on upper layer request.
- **IPSec Provisioing & IPSec Proxy**. Developed by DELTA.
  - IPSec Provisioning Manager, controls and manipulates IPSec tunnels through the use of IETF IPSec Provisioning Policies.

All these objects are described below in the paragraph for each layer.

3.1 VPN Service Configuration Building Block

The VPN Service Configuration building block is responsible for two things:

- **Interface to VPN services**. The management functions are based on [M.3208.3] and [M.3108.3]. The provided services are for creating, modifying and deleting VPN service and VPN connections.
- **Virtual topology**. A described above, the virtual topology uses three key concepts for describing the topology of a VPN. This topology is constructed and maintained through the management functions available to the VPN user.

Providing the interface to the VPN services results in another responsibility:

- **Managing the work-flow of VPN operations**. As shown in the Figure below, the work-flow for the VPN-SC high-level management functions form the base for the VPN-P’s work-flow.

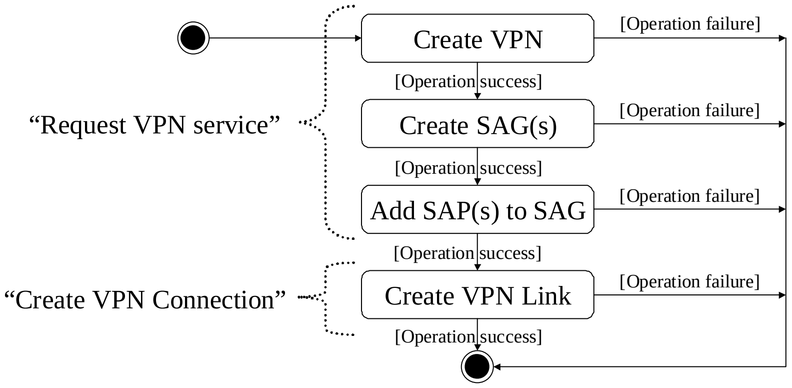

Figure 6 VPN workflow

3.2 VPN Provisioning Building Block

As defined earlier the IP VPN service components developed in FORM project focus on provisioning and configuration aspects of the service. The VPN Provisioning Building Block is defined as a middle layer aiming at mapping information received from the higher layer (sent by a VPN customer via the VPN-SC BB), to the lower part, i.e. network layers involve in implementation of IP tunnels (IPSec-P and GQIPS BBs). This mapping is done also the other way around, when providing information or notification from the network level to the service and customer level.

The role of the VPN-P BB is not just restricted to the mapping of the information, from some virtual level to network one. It is also to answer as best as possible to VPN customer requests based on available network resources and a main constraint is to provide this service dynamically. It could be, therefore, defined as a mediation process between service request and network resources.

Based on user requirements, defined above, and available standards or work studies, a set of principles have been defined allowing to build the architecture of the component:

- As main role of the component concerns the mapping between different logical view a layered approach seems well-adapted. Three levels are defined:
    - ***Virtual Topology view***: at this level an interface with the VPN-P client is provided, and objects managed are VPN, SAG, SAP, VPNLink, etc … (see figure Virtual Topology of the VPN Service)
    - ***Abstract Tunnel and Real Network Topology view***: the abstract tunnel concept is based on the idea of defining end-to-end link between two or more VPN end users from an abstract point of view. The aim is to map the virtual or end user view to a level non technology specific, through definition of generic tunnel parameters which can be applied to different specific technologies. The Real Network Topology defines the necessary entities for building end-to-end connections, including Border Nodes (CPE and Provider's), StubLink and Network Interfaces.
    - ***Tunnel Factory***: this object interacts with specific entity dedicated to the set up of tunnel. It is therefore, in charge of requesting tunnel creation and activation and passing all necessary parameters to configure the tunnel to the network level. These network level entities are defined as plug-in of the VPN-P. Thus it allows to create, from the VPN-P, tunnels based on different IP tunnelling mechanisms (IPSec, MPLS, L2TP) or IP mechanisms able to guarantee QoS on an end-to-end connection (Bandwidth Broker, DiffServ). One possibility is also to mix different IP tunnelling mechanism for one VPNLink, allowing to provide security features as well as guaranteed QoS.

- Interface provided to the VPN-P client is defined based on ***ITU-T draft standard M.3208.3*** [ITU-T M3208.3], which main focus is on the VPN service management.
- One main innovative aspect of the VPN-P is to support a ***dynamic mapping between user requirements to network configuration***. User requirements are expressed in the form of ***Service Class*** identifying the type of service (e.g. VoIP), the quality level (e.g. Premium) as well as security level (e.g. secret). This end user Service Class is then mapped to abstract Service Classes, which are divided into two main components: one for QoS and one for security. At the abstract level parameters are non technology-specific (e.g.: for security the following parameters are defined: authenticity, confidentiality and integrity). From this level, when creating the physical tunnel, the abstract Service Class is mapped to technology specific parameters, it means to be used at network level for implementation of the tunnel. All information contained in Service Classes can be configured by the VPN SP, and, in addition VPN SP can also define the service class mapping process thanks to the use of policy.

- The VPN-P component needs to take decisions at several places during a tunnel creation process:
    - Choice of the protocol combination that will be used for the IP tunnel.
    - Computation of the Service Class used to configure the service.
    - Sub-process flow depending on the two previous decisions for the tunnel creation process.

  These decision processes should be configurable dynamically by the VPN-P administrator. The VPN-P component integrates a ***business processes policy framework*** that follows the previous recommendations. This framework is object-oriented and not agent-oriented. It falls into two parts:

    - A generic upper layer that is to say not dependant on the implementation of the policy engine and corresponding to the implementation of the policy framework developed by FORM.
    - A lower layer implementing a policy engine, that implements methods of the upper layer. Implementation of such policy engine component is already available on the market.

The VPN-P BB includes also an ***administrative console*** allowing the VPN SP administrator to:

- Customise the VPN service regarding the evolving context, through the use of policy,
- Configure VPN resources,
- Visualise all VPN service interactions and resources.

3.3 IPSec Provisioning Building Block

IPsec protocol suite [IETF RFC2401] provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more "paths" (i.e tunnels) between a pair of hosts, a pair of security gateways (the term security gateway refers to an intermediate system that implements IPsec protocols, e.g., a router or firewall implementing IPsec), or between a security gateway and a host.

The set of security services that IPsec can provide includes access rejection of replayed packets (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality and authentication of end-points. Because these services are provided at the IP layer, they can be used by any higher layer protocol, e.g., TCP, UDP, ICMP, BGP, etc.

IPsec uses two protocols to provide traffic security:

- Authentication header (AH) [IETF RFC2402], which provide connectionless integrity, data origin authentication, and an optional anti-replay guard.
- Encapsulating security payload (ESP) protocol [IETF RFC2406], which provides confidentiality (encryption), and limited traffic-flow confidentiality. It also may provide connectionless integrity, data origin authentication, and an anti-replay service.

AH and ESP are vehicles for integrity/confidentiality, based on the distribution of cryptographic keys and the management of traffic flows relative to these security protocols. (Only ESP encapsulation was supported by the FORM trial implementations with IKE key exchanging [IETF RFC2409])

These protocols may be applied alone or in combination with each other to provide a desired set of security services in IPv4 and IPv6. Each protocol supports two modes of use: transport mode and tunnel mode. In transport mode the protocols provide protection primarily for upper layer protocols, in tunnel mode, the protocols are applied to tunnelled IP packets. The latter was supported by the FORM IPSec-P Building Block prototype.

IPSec protocols themselves are standardised and stable, but how to configure IPSec on a more practical level is less so. Though the IETF IP Security Protocol Working Group has been responsible for the standardisation of the IPSec RFCs, only IPSec monitoring MIBs (eg. to support SLA-Assurance) are in development and still in draft.

However, in the IP Security Policy Working Group you find the most progressed (but also still in drafts and ever-changing) work on configuration via Policy Provisioning.

The main function of the IPSec-P Building Block can be summarised to:

- Provide a (pre-)standardised interface to IPSec Provisioning through the use of Policies
- Receive Request from the IPSec-P user for initial configuration of Enforcement Points.
- Receive IPSec Provisioning Policies [IETF IPSec Conf, IPSec Policy] describing the required IPSec security level
- Receive IPSec Provisioning Policies describing the tunnel end-points and filtering options.
- Validate and stores these policies and make them available for download to Enforcement Points.
- Ensure that the Policies are pushed to relevant Enforcement Points in a standardised way. (E.g. through the uses of COPS/COPS-PR. The latter was not fully implemented in the BB)

To do this the IPSec-P Building Block provides a versatile interface to IPSec provisioning and thus allows the IPSec-P user to alter many different IPSec related parameters and group them into various service offerings. The IPSec-P Building Block was specifically designed this way to be potentially useful (reused) in other contexts.

Initially the work in IETF IP Security Policy (IPSP) Working Group was influential for the specification of the IPSec-P BB. The draft on the Security Policy Specification Language (SPSL) [IETF SPSL] also formed the basis of the XML Schema defining the policy objects to be passed from VPN-P BB to IPSec-P BB.

SPSL is a vendor and platform independent language for specifying communication security policies, especially those controlling the use of IPSec and IKE protocols. SPSL allow the security policies to be specified in an interoperable language, stored in common databases and processed by management systems separate from the security devices. However, SPSL's notion for textual policy object representation (signed files) did not match the goal to have XML as a common basis for BB interactions. The conversion from the SPSL specification to an appropriate XML Schema was performed manually and only a subset of SPSL was expressed as an XML Schema. This provided the basis for the first VPN-P IPSec-P BB interactions. However, as work in the IPSP Working Group was focussing on core models prior to deriving languages, it was decided to drop the IPSec-P reliance on SPSL (the draft also expired) and focus more on [IETF IPSec Conf, IPSec Policy]. The gain was better compliance with emerging IETF standards and improved expression capabilities, but the downside was the loss of integral security concepts like 'Maintainer', defining who - authenticated via signatures - were allowed perform CRUD (Create/Read/Update/Delete) operations on the policies. Removing these types of objects indicates that the security mechanisms would be depending on the technology used to access the BB. As XML was used for describing and passing objects between the VPNS BBs work in the IETF XML Digital Signatures Working Group is relevant. This WG has the task to develop an XML compliant syntax used for representing the signature of Web resources and portions of protocol messages (anything referencable by a URI) and procedures for computing and verifying such signature, providing integrity, authentication, and/or non-repudiatability. Applying this to BB interactions would provide a standardised way of controlling access to all BBs in the VPNS and not just to the IPSec-P part. This was not implemented due to time constraints.

Also the KeyNote Trust-Management system [IETF RFC2704] was looked at, as a candidate for security policy specifications, but it was deemed to generic (high-level) for the (low level) Network Provisioning required by the Building Block.

An interesting effect was encountered in the division of tasks between the VPNS building blocks concerning the topology. The VPN-SC was to maintain the VPN topology, the VPN-P was to maintain the virtual tunnel mappings and the IPSec-P should provide actual IPSec-P tunnels. This indicated that the VPN-P layer mostly required the IPSec-P layer to create IPSec SA's between end-points, for which a simple interface could be used. However, as the IPsec-P BB was also designed with re-usability in mind a more versatile interface was specified closer to the standardised concepts of IPSec/Ike-Associations, Rules, ESP-Transforms, etc.

The negative side effect of having a versatile interface for the IPSec-P BB, thus resulted in more complicated interactions than actually required to support the functionality needed by the VPN-P BB.

In the implemented trial system the VPN-P layer is required to perform the entire mapping to IPSec-P concepts of IKE/IPSec associations, IKE/IPSec rules, etc. when basically a 'provide-ipsec-link-between-two-endpoints' was required. Upon examination, it did not seem possible to circumvent this, without 'pushing' topology information further down into the IPSec-BB.

To keep the IPSec-P versatility and at the same time alleviate the VPN-P from some of the mappings, another 'glue'-BB could have been placed between the VPN-P and IPSec-P level. This approach would still fit nicely with the FORM ODF principles of bundling BBs together in a BB Set to obtain desired functionality.

Several considerations were made on the mappings between high-level information presented to the VPN-SC/VPN-P and the low-level aspects of the IPSec-P. E.g. it was identified that the Service Class abstraction used by the VPN-P/VPN-SC level should contain a 'Security Component' specifying the intended security level of the requested tunnel regardless of tunnel paradigm.

These generic Service Class parameters suggested for the Security Component are:

- Security Level : Textual

- Authentication : Boolean
- Data Encryption : Boolean
- Anti Replay : Boolean
- Authentication & Encryption : Boolean

The 'Security Level' would describe things like "High-Security", "No-Security", etc., for VPN-P/VPN-SC users, but with a qualifying description like*: "High-Security uses the XXX Algorithm with YYY Key length and provides protection between Provider network and Customer Premises Equipment......*". However, this 'qualifying description' will indirectly relate to the VPN technology (or tunnel paradigm used) as it is difficult to describe or qualify 'High Security' without relating to technological aspects (like VPN architecture, encryption algorithms, key length, etc).

It was interesting to see that a few parameters like Authentication, Encryption, etc, were sufficient to describe a high-level security status of a VPN service together with some additional qualification. E.g. could VPN architecture be important to some users. Are you using MPLS? Is the data encrypted on the last hop from Provider Edge to Customer Network?

If the Security Component contains a technology mapping, the VPN provider can change the technology mappings over time as new VPN paradigms/technologies emerges and the state of crypto-analysis changes.

In summary the mappings should cover three components at least:

1) A non-technical Top Level Classification which most can relate to with a minimum of description. The top-level classification could relate to classification of the information traversing the VPN, e.g. by using the classic RFC1108/E.O. 12958 U.S. levels) [IETF RFC1108].
   - *Top Secret* - This level should be applied if the unauthorised disclosure of the information would cause exceptionally grave damage to VPN Service Users. ('Top Secret' would probably use multiple technologies)
   - *Secret* - This level should be applied if the unauthorised disclosure of the information would cause serious damage to VPN Service Users.
   - *Confidential* - This level should be applied if the unauthorised disclosure of the information would cause damage to VPN Service Users.
   - *Unclassified* - This level should be applied if the unauthorised disclosure of the information would cause no damage to VPN Service Users.
2) A set of generic security parameters. (We operated with three: Authetication (boolean), Integrity (Boolean), Confidentiality (Boolean), as Integrity also include AntiReplay and Authentication+Confidentiality=AuthenticationEncryption, which must be qualified in the technology mapping section.
3) A Technology Mapping. Without a technology description for the actual technology mapping chosen (E.g. IPSec), the Top-Level, sub-classification and generic security parameters make little sense. It would describe key elements of the security aspects used in the provisioning (Algorithms, key lengths, VPN architecture, etc)

It is the VPN-P layer that exclusively decides on how mappings are performed.

4 Conclusion

This paper presents IP VPN service in a B2B context. VPN is recognised as an essential enabler for B2B. VPN market as well as studies from different standardisation bodies and forum are today focusing more and more consideration. However, we consider the market as still open and standardisation results not mature. VPN Working Group, from the FORM project, demonstrated from a top down approach that organisations, as well as Service Providers, are expecting really innovative solutions able to support B2B.

The VPN building blocks developed by the FORM partners have been validated through trials. Even if these components are still at prototype stage, they allowed to evaluate benefits of such solution based on innovative principles. Development of these building blocks followed methodology guidelines and principles defined by the FORM ODF (see [formD9] and [formD12]), main benefits of such approach insures openness and reusability of each of the components. At last, state of the art technologies such as J2EE (EJB, JMS) and XML have been used efficiently and benefits of such technologies and some others have been evaluated within the FORM project (see [formD10]).

Each partner of the VPN Working Group will reuse results of the FORM project, mainly own components they have developed. Possibility to exploit these results by providing innovative solution on the market will be evaluated. However, some of these components will be reused in other R&D projects. Specifically there will be possibility for one partner to adapt some of the VPN components to 3G environment and therefore to support mobile users in a Virtual Home Environment.

This paper tried to provide mid-term vision on VPN service in the evolving telecommunication context. In the FORM project we considered dynamic configuration and activation of VPN service based on end user requirement as an essential evolution for VPN service. Next step should allow to transparently fulfilling end user requirements based on end user context and to regroup configuration and activation phase into one and therefore to get instant VPN service. Providing end user with the possibility to use as efficiently as possible network resources, in a transparent way, is a main trend today in telecommunications world.

5 References

[formD9] Leray, Eric, “D9: Final FORM Framework”, IST-1999-10357/WIT/WP3/1019, February 2002.

[formD10] Quinn, Niamh, “D10: Validation of Inter-Enterprise Management Framework”, IST-1999-10357/BRI/WP5/02xx, due February 2002.

[formD12] Wade, Vincent, “D12: Guidelines for Co-operative Inter-Enterprise Management”, IST-1999-1057/TCD/WP3/012, February 2002.

[IETF RFC2401] IETF, RFC 2401 (Security Architecture for the Internet Protocol).

[IETF RFC2402] IETF, RFC 2402 (IP Authentication Header).

[IETF RFC2406] IETF, RFC 2406 (IP Encapsulating Security Payload).

[IETF RFC2409] IETF, RFC 2409 (The Internet Key Exchange (IKE)).

[IETF RFC1108] IETF, RFC 1108 Security Options for the Internet Protocol

[IETF IPSec Conf] IETF Draft v/2: “IPsec Configuration Policy Model

[IETF IPSec Policy] IETF Draft v/2: "IPSec Policy Information Base

[IETF SPSL] IETF Draft Security Policy Specification Language] (expired)

[IETF RFC2704] IETF RFC: The KeyNote Trust-Management System Version 2

[IETF IPVPN] IETF Draft: IP VPN Policy Information Model

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

[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”

[OConn00] M.O.Connell, P.Nixon, ”Next Generation Business to Business E-Commerce” EC&WEB , Sept, 2000

[Sand00] M.Sanders, B.Temkin, ”Global eCommerce Approaches Hypergrowth”, Forrester Report, April 2000. www.forrester.com