IP Virtual Private Networks

IP Virtual Private Networks Security’’

Editor: Christian Garbrecht, T-Systems Nova GmbH, DT

Suggested readers
Product managers, network designers, people involved in the deployment, operation and management of IP-VPNs, equipment vendors.

Abstract
This document provides recommendations on IPVPN security. The aim is to explain the problems, to identify standardisation gaps and to provide solutions whenever possible. It provides a description and proposes solutions related to the following items:

• Identification and authentication of the IPVPN components;
• Identification and authentication of remote (e.g. mobile) users;
• Public Key infrastructure for IPVPN components;
• Security and key distribution of multicast within IPVPN;
• Inter-working of IPSec with tunnelling protocols (e.g. MPLS).
Eurescom PARTICIPANTS in Project P1107 are:

- Deutsche Telekom AG
- Elisa Communications Corporation
- France Télécom
- MATÁV Hungarian Telecommunications Company Ltd
- Hellenic Telecommunications Organization S.A. (OTE)
- Portugal Telecom, SGPS, S.A

IP Virtual Private Networks
Deliverable D2 “IP VPN Security”
Editor: Christian Garbrecht, DT
Project leader: Jorge Carapinha, PT
Project supervisor: Valerie Blavette, Eurescom GmbH
Eurescom published project result; EDIN 0300-1107
© 2002 EURESCOM Participants in Project P1107

Disclaimer

This document contains material which is copyright of certain Eurescom PARTICIPANTS and may not be reproduced or copied without permission. The information contained in this document is the proprietary confidential information of certain Eurescom PARTICIPANTS and may not be disclosed except in accordance with Section 5 of Eurescom’s general conditions of the contract.

The commercial use of any information in this document may require a licence from the proprietor of that information.

Neither the PARTICIPANTS nor Eurescom warrant that the information contained in this document is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using the information.
Preface

The IP-based Virtual Private Network (IP VPN) has emerged as one of most promising services for network providers.

However the widespread deployment of IP VPNs has been delayed by the lack of interoperable implementations and confusion over the high number of solutions that are described by the term IP VPN. Indeed several challenges like security, quality of service or scalability are associated with the implementation of VPNs over IP-based networks. A wide variety of models and network solutions have been proposed by the networking and telecommunications industries to deal with these requirements.

It is crucial to get a global picture and understand the strengths and shortcomings of all the available tools and network solutions and related interoperability problems. Therefore, the approach followed by the EURESCOM P1107 project is as wide-ranging as possible, without any bias towards a specific technology or architecture.

The network operators, through EURESCOM, should play an active role in this area, in order to promote interoperable, flexible and secure IP VPN implementations.

This project report is the second from the project and focuses on IP VPN security issues.

This project had 6 participating companies and a budget of 85 man months.
Executive Summary

Why you should read this project report

IP-based VPNs are very common nowadays. A number of different concepts and strategies to establish them exist and are already offered by some network service providers. However there are still some special usage scenarios that are not covered by generic VPN offers, neither are they explained in the common literature.

The benefit for your company

Since this report includes conceptual work as well as verification results from lab experiments, it addresses product managers and network designers as well as network operating staff. Equipment vendors may also use this document to learn how they can enhance their equipment to support the addressed functionality.

Aspects addressed by this project report

Three aspects of IP-VPN design are addressed by this document:

- Inter-working of the two most common IP-VPN technologies namely MPLS and IPSec
  
  MPLS and IPSec are evaluated in a test-bed with respect to the standard requirements of VPNs, concepts, and how and why both technologies may be combined.

- Remote access and seamless mobile access via 3rd party ISPs
  
  Two different implementations were compared to learn how they realise a PKI with automatic IPSec initialisation. Concepts for the chain of trust, in the case where more than one certification authority is involved, are introduced. In order to support seamless mobility and secure remote access, configurations for different communication scenarios are introduced and proved against in a threat analysis. Realisation concepts to satisfy these scenarios are given.

- Key management for closed user group multicast scenarios such as Internet Pay TV
  
  Typical multicast applications and services are introduced and sorted according to the following properties: logical network topology, group characteristics, traffic characteristics and special security requirements. Multicast security concepts are developed and requirements for an IPSec implementation suitable for securing multicast transmissions are defined. Finally, an implementation of a demonstrator providing multicast security over IPSec is presented.

Conclusions

In this project a group key management architecture was specified and implemented successfully. This architecture is in line with the official IETF architecture proposal [11], [16]. Since different usage scenarios require different network capabilities, for the demonstrator “pay-per-month a/v streaming” was applied. Despite the successful implementation a number of unsolved problems such as reliable re-keying, Security Association synchronisation, member exclusion in scenarios with a short-term member verification (e.g. pay-per-minute) or compatibility with ISAKMP still exist.

Supporting remote access via IP-VPN needs some authentication and authorisation mechanisms which are recommended to be certificate based. Certificates can be sent in-band or out-of-band. Two different protocols representing respectively an in-band and out-of-band solution for an automatic initialisation of IPSec, are evaluated and compared.

Similar to a multicast environment, for seamless mobile access, a number of different usage scenarios exist. Here four different scenarios are analysed. As a result there is no overall architecture that satisfied all requirements, but compromises have to be considered in order to get an acceptable solution. This gives the opportunity to be compatible with 3G all-IP networks (and 4G) from the beginning.

The results of the MPLS/IPSec inter-working tests demonstrate that MPLS based VPN networks have nearly reached the security-feature level of a layer 2 based VPN.

Today, IPSec is the most secure, best supported and most flexible technology to fulfil the requirements of data confidentiality, integrity, authentication and replay detection within a VPN. The IPSec and the MPLS technologies can be combined very satisfactorily to build good, secure and well-manageable VPNs from the point of view of the customer and service provider.
List of Authors

Erik Neumann, Jörg Schwenk, Bernhard Löhlein, Tobias Martin, Frank Burkhardt, Christian Garbrecht (Deutsche Telekom AG)
Miika Malinen (Elisa Communications Corporation)
Pierre Cazenave, Eric Delacour, Dominique Alglave & Mohamed Achemlal (France Télécom)
Luis Azevedo, Carlos Sarabando (Portugal Telecom)
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>3</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>List of Authors</td>
<td>5</td>
</tr>
<tr>
<td>Table of Contents</td>
<td>6</td>
</tr>
<tr>
<td>Abbreviations</td>
<td>7</td>
</tr>
<tr>
<td>Definitions</td>
<td>9</td>
</tr>
<tr>
<td>1. Introduction</td>
<td>10</td>
</tr>
<tr>
<td>1.1 Objective of this document</td>
<td>10</td>
</tr>
<tr>
<td>1.2 Investigated Security Issues</td>
<td>10</td>
</tr>
<tr>
<td>2. IPSec Key Management for Multicast Transmission</td>
<td>12</td>
</tr>
<tr>
<td>2.1 Multicast Security Requirements and Concepts</td>
<td>12</td>
</tr>
<tr>
<td>2.1.1 General Security Tasks</td>
<td>12</td>
</tr>
<tr>
<td>2.1.2 Key Establishment</td>
<td>12</td>
</tr>
<tr>
<td>2.1.3 Standardisation</td>
<td>15</td>
</tr>
<tr>
<td>2.2 Multicast Applications and Services</td>
<td>15</td>
</tr>
<tr>
<td>2.2.1 Demonstrator</td>
<td>16</td>
</tr>
<tr>
<td>2.2.1.1 Scenario Pay-per-month a/s streaming</td>
<td>16</td>
</tr>
<tr>
<td>2.2.1.2 Software Design / Implementation Tasks</td>
<td>16</td>
</tr>
<tr>
<td>2.2.1.3 Standardisation Gaps</td>
<td>17</td>
</tr>
<tr>
<td>3. IPVPN Components and Remote Users</td>
<td>19</td>
</tr>
<tr>
<td>3.1 Technical Issues Related to Remote Access</td>
<td>19</td>
</tr>
<tr>
<td>3.2 Smart Card based Remote Access</td>
<td>20</td>
</tr>
<tr>
<td>3.3 DKI applied to Remote User Scenarios</td>
<td>21</td>
</tr>
<tr>
<td>3.4 Usage of PKI to Automatically Initialise IPsec</td>
<td>23</td>
</tr>
<tr>
<td>3.4.1 CMP protocol description</td>
<td>23</td>
</tr>
<tr>
<td>3.4.2 SCEP Protocol Description</td>
<td>24</td>
</tr>
<tr>
<td>3.4.3 Comparison Between the Protocols</td>
<td>24</td>
</tr>
<tr>
<td>4. Remote Users via Mobile IP</td>
<td>25</td>
</tr>
<tr>
<td>5. Inter-working of Security Technologies</td>
<td>25</td>
</tr>
<tr>
<td>5.1 Security in VPN Architectures</td>
<td>29</td>
</tr>
<tr>
<td>5.1.1 Risks and security Requirements</td>
<td>29</td>
</tr>
<tr>
<td>5.1.2 Risks and Vulnerabilities for Different VPN Models</td>
<td>29</td>
</tr>
<tr>
<td>5.1.3 Countermeasures</td>
<td>30</td>
</tr>
<tr>
<td>5.2 MPLS-based VPNs and IPsec Inter-working Scenarios</td>
<td>30</td>
</tr>
<tr>
<td>5.2.1 Secure Remote Access (CE-PE-Scenario)</td>
<td>30</td>
</tr>
<tr>
<td>5.2.2 IPsec Tunnels Across SP Networks</td>
<td>31</td>
</tr>
<tr>
<td>5.2.3 End-to-End IPsec Tunnels</td>
<td>32</td>
</tr>
<tr>
<td>5.2.4 IPsec Tunnels Between SP Networks</td>
<td>35</td>
</tr>
<tr>
<td>6. Test and Demonstration</td>
<td>35</td>
</tr>
<tr>
<td>6.1 Testbed Implementation</td>
<td>35</td>
</tr>
<tr>
<td>6.2 Tests Definition</td>
<td>34</td>
</tr>
<tr>
<td>6.3 Test Results and Recommendations</td>
<td>35</td>
</tr>
<tr>
<td>7. Conclusion</td>
<td>36</td>
</tr>
<tr>
<td>References</td>
<td>37</td>
</tr>
</tbody>
</table>
Abbreviations

AH Authentication Header
API Application Programming Interface
ATM Asynchronous Transfer Mode
BGP Border Gateway Protocol
CA Certification Authority
CE Customer Edge (router)
CMP Certificate Management Protocol
CN Correspondent Node
CRL Certificate Revocation List
EIGRP Enhanced Interior Gateway Routing Protocol
ESP Encapsulation Security Payload
DHCP Dynamic Host Configuration Protocol
DMZ De-Militarised Zone
DoS Denial of Service
FA Foreign Agent
FW Firewall
GKM Group Key Management
HA Home Agent
IETF Internet Engineering Task Force
IKE Internet Key Exchange
IPAS Internet / Core Perspective Attacks
ISAKMP Internet Security Association and Key Management Protocol
KDC Key Distribution Centre
KEK Key Encryption Key
L2TP Layer 2 Tunnelling Protocol
MIP Mobile IP
MN Mobile Node
MPLS Multi-Protocol Label Switching
MSEC IETF Multicast Security Working Group
NAPT Network Address and Port Translation
NSP Network Service Provider
OPA Outside / Customer Perspective Attacks
OSPF Open Shortest Path First
PE Provider Edge (router)
PKI Public Key Infrastructure
POP Point Of Presence
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>RA</td>
<td>Registration Authority</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>RTP</td>
<td>Real Time Protocol</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SAD</td>
<td>Security Association Database</td>
</tr>
<tr>
<td>SCEP</td>
<td>Simple Certificate Enrolment Protocol</td>
</tr>
<tr>
<td>SG</td>
<td>Security Gateway</td>
</tr>
<tr>
<td>SPD</td>
<td>Security Policy Database</td>
</tr>
<tr>
<td>SP</td>
<td>Service Provider</td>
</tr>
<tr>
<td>SPI</td>
<td>Security Parameters Index</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TCP</td>
<td>Transport Control Protocol</td>
</tr>
<tr>
<td>TEK</td>
<td>Traffic Encryption Key</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UDP</td>
<td>Unified Data Protocol</td>
</tr>
<tr>
<td>VCI</td>
<td>Virtual Circuit Identifier</td>
</tr>
<tr>
<td>VPI</td>
<td>Virtual Path Identifier</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
Definitions

VPN
A VPN can be defined as a service in which customer connectivity amongst multiple sites is deployed on a public or shared infrastructure with the same access or security policies as a private network. A VPN should be comparable to a private network in performance, reliability, management security and Quality of Service (QoS). Customers of VPN services use shared facilities and equipment, which are managed, engineered and operated by a public network operator, either totally or partly.

IP VPN
An IP Virtual Private Network (IPVPN) can be defined as a VPN implementation that uses public or shared IP network resources to emulate the characteristics of an IP-based private network. (Note: since the focus of this document is IP-based VPNs, the terms VPN and IPVPN are used interchangeably in most cases).

Protection Objectives Defined
In order to make an analysis of the protection needs of elements in the Network, first we need to define the objectives of such efforts. For the Scenarios described in the following chapters, the Protection Objectives are:

1. **Confidentiality**: Service Information must, at all times during the Transmission and Storage processes, be protected from unauthorised viewing and access.
2. **Integrity**: Unauthorised or unintentional manipulation or falsification of data and systems must be prevented.
3. **Authenticity**: It must be possible to obtain the origin or source of the Data packets received.
4. **Availability**: System functionality must be constantly available.

Risk Assessment
The risk regarding damage level and damage frequency rises, whenever it is possible for a given Threat to endanger one of the Protection Objectives. In order to keep the focus on prevention of any intolerable risks, a granular assessment has been made of the damage risk for each Scenario.

The following three levels of risk appraisal were used to describe the possible effects of singular threats:

- **Risk of little consequence** - to the sequence of communication. This means that although unauthorised parties could intercept certain information, said information has a very low damage potential.

- **Tolerable Risk** – a risk, which would allow a higher level or frequency of damage to occur. The expected maximum damage and the ensuing consequences are calculable, and are under certain circumstances seen as being acceptable.

- **Intolerable Risk** – a risk containing the possible threat of damage that could put a User or Company in danger of losing the necessary means of existence. For instance, the theft or manipulation of highly sensitive data belonging to one of the communication system participants could bring about such an occurrence.

The assessment of the risk of damage, using the same network elements, may differ in each scenario. The basis for the risk assessment is formed from the worst-case scenario. It would be sensible for participants, who are aware of the fact that, for instance, all involved communication elements can be found in the Internet and no information is available as to the security of these elements, *not* to transfer any sensitive data or information using said elements. Therefore, at this point there is a tolerable, but no intolerable risk.

Another example would be the communication between one element protected inside the Intranet and another element outside the protected environment, in the Internet. It can be assumed here that sensitive information may be found on the element inside the protected Intranet, which could be compromised or manipulated during communication with the element in the Internet, possibly leading to intolerable damage. A possible threat to the communication, therefore, poses an intolerable risk.
1 Introduction

1.1 Objective of this document

The objective of this document is to give a high-level overview of the goals and results of the three special IP VPN usage scenarios not covered by general VPN offers and not explained in the common literature:

- Security of multicast within IPVPN, including the set-up of a small-scale demonstrator for IPSec multicast key management and encryption.
- Identification and authentication of remote users for legacy and Mobile IP-based remote access;
- Interworking of IPSec with tunnelling protocols (e.g. MPLS, Mobile IP);

Since this report includes conceptual work as well as verification results from lab experiments, it addresses product managers and network designers as well as network operating staff. Equipment vendors may also use this document to learn how they could enhance their equipment to support the functionality addressed.

1.2 Investigated Security Issues

IP-based VPNs are very common nowadays. A number of different concepts and strategies to establish them exist and are already offered by some network service providers (NSP). Deliverable D1 of this project reflects the definitions and specifications of the different approaches and gives a number of recommendations and guidelines in order to ease the development of a VPN service strategy for an NSP.

Besides general VPN architecture issues, there are special usage scenarios worth investigating in more detail:

A VPN is not only a mapping of a business relationship inside a company (corporate VPN) or in a business-to-business scenario, but can also be a mapping of an intra-community relationship, where information should be spread out to many people in parallel. IP television provisioning is a good example. If a large number of participants are involved in such a scenario, it leads to the question, how can IP multicast be used to support VPNs? Within this project, typical multicast applications and services are introduced and classified against the following properties: logical network topology, group characteristics, traffic characteristics and special security requirements. Multicast security concepts have been developed and requirements for an IPSec implementation, suitable for securing multicast transmissions, have been defined. Finally, an implementation of a demonstrator providing multicast security over IPSec is presented. The architecture of the demonstrator was presented in August 2001 at an IETF meeting in London. The detailed results can be found in [2].

Business processes adapt more and more to the mobility paradigm of western societies. Workplaces are outsourced to tele-workers, business travellers have to be reachable even on the road and have to access company data from remote places around the globe. Usually, remote access takes place via dial-up to the company’s dial-in-router. Network security issues are handled by the telephone network. For international calls particularly, this can create high costs that may be avoided, if the service of a local 3rd party dial-up provider can be used. Also, it is not very practical to have a transmission rate of 56k maximum. New access media like wireless LAN, UMTS and xDSL can offer a number of new services in order to get a transparent IP connection, wherever the user is. To make the different access technologies transparent to the user and to give him the IP connectivity he is used to having in his home office, the Mobile IP protocol suite may be applied. This deliverable shows how chip-cards can be applied to secure user authentication, what implications that has for a PKI if remote users are connected via the public internet and how Mobil IP, in combination with IPSec, can offer a seamless mobile IP-VPN solution. Detailed results can be found in [3].

Since VPNs naturally are not bound to geographic regions (e.g. countries, continents), they may involve more than one NSP. These do not necessarily offer the VPN service based on the same technology. Some use IPSec, some MPLS, some may offer layer-2-based VPNs. In order to create a homogeneous End-to-End VPN for a customer, these methods have to inter-operate, respecting at least a strict VPN segregation over all provider networks. The project approaches the main security issues in the VPN context focusing on MPLS and IPSec technologies. The results produced include analyses for single domain MPLS security, inter-
domain MPLS security and the IPSec/MPLS combination. Finally these analyses were proven by establishing, executing and evaluating test scenarios. The detailed results can be found in [4].

There might be other scenarios worth investigating but due to limited resources and the background knowledge of the consortium, this project focused on the three topics introduced above. They were chosen, since they are very relevant to the developing VPN market. Internet TV is very intensively discussed, at least in Germany. Security and multicast issues have to be solved, before Internet TV can take off. Common market analyses say that over 70% of the VPNs will be remote-access based. Solving the technical problems will answer the short term market requirements. Last, but not least, a number of carriers and ISPs already have a MPLS- or an IPSec-based VPN product in their portfolios or will have it this year. Ensuring a customer-oriented end-to-end service, even across provider borders, is the main driver for the inter-operation investigations in this project.
2 IPSec Key Management for Multicast Transmission

IP multicast allows conservation of bandwidth when the same content is sent to multiple receivers. IPSec is a well-known protocol to secure unicast IP traffic between peers or sites. It has been standardised by the IETF (see [6]). But IPSec is not suitable for IP multicast, because securing traffic that is sent to more than one destination requires new methods and fundamental extensions.

Regarding multicast, the character of VPN is determined by means of closed user groups, identified by a common service subscription. The separation of these closed user groups is handled by means of IPSec.

2.1 Multicast Security Requirements and Concepts

The security requirements of unicast-based services and multicast-based services are almost identical. For encryption and authentication of multicast traffic, proven protocols like ESP (see [8]) and AH (see [7]) can be used. But regarding the key establishment, the solutions to meet these requirements may be quite different. Typically, the proposed multicast solutions take the unicast solutions as a basis and extend them as required. In the long term, unicast algorithms will be regarded as simplifications of multicast algorithms that are developed today.

2.1.1 General Security Tasks

**Authentication** is done only once for each participant. Therefore, asymmetric encryption schemes can be used via unicast connections. Typically, certificates are exchanged. For multicast, it is meaningful to set up a central entity that allows group members to authenticate and to receive the initial key upon success. In single sender scenarios, this central entity is often combined with or at least co-located to the sender. In scenarios involving multiple senders (conferencing), the selection of a sender is artificial.

**Confidentiality** requires encryption. Traditional unicast protocols like ESP can be used for multicast as well. Even for unicast, asymmetric encryption schemes are not used, because of the computational overhead. In the case of multicast, asymmetric encryption schemes are not meaningful, because they would require that the traffic be encrypted differently for each destination.

**Integrity** may be checked by means of a signature. Traditional unicast protocols like ESP and/or AH can be used for multicast as well. A symmetric algorithm only assures, that the message was sent by an entity that knows the symmetric key, i.e. a group member. In unicast scenarios, this is not a problem, because apart from the indicated sender, the receiver is the only entity that knows the key. But a multicast service that requires the authentication of the sender needs to implement an asymmetric scheme, or a different key has to be used for each sender (multiple multicast sessions).

**Connection Management** depends on the protocol in use. For IPSec it is done via the Security Association Database (SAD). Some unicast protocols like IPSec allow peers to negotiate the security parameters during connection set-up. One important parameter is the connection ID, called the Security Parameters Index (SPI) in IPSec. Multicast does not allow for the negotiation of parameters, because a member may join at any time. The receiver cannot assign the connection ID. Regarding IPSec, this requires slight changes in SPI assignment and evaluation for multicast Security Associations (SA).

2.1.2 Key Establishment

The differences between unicast and multicast security tasks, mentioned in the previous subsection, are minimal. But confidentiality and integrity require a key to be known by all senders and receivers. The fact that the key has to be established at more than two entities is the main difference regarding the security of unicast and multicast. Therefore, the solutions for key establishment are quite different. Typically, the proposed multicast solutions take the unicast solutions as bases and extend them as required. In the long term, unicast algorithms will be regarded as simplifications of multicast algorithms that are developed today.

The effort required for key establishment depends on the scenario, i.e. on the lifetime of a multicast group, on the number of group members (receivers or senders), on the fluctuation, and on whether former members need to be excluded. These parameters define how often the keys have to be replaced. In simple scenarios, re-keying may be unnecessary.
The costs for key establishment can be measured by the computational overhead or by the number of packets to be exchanged. For simple scenarios like online lectures, no re-keying is necessary, i.e. there are no additional costs for re-keying. On the other hand, a complicated scenario like global pay-per-minute a/v streaming, requires frequent re-keying. While the simple scenarios can already be solved, there is currently no practical approach for the most complicated scenarios, because the costs are simply too high.

A pre-shared key is not meaningful for a real service, especially not for a large number of recipients as is the situation for multicast services. There are two different approaches to key establishment remaining: key transport (key distribution) where a central entity defines a key and transmits it to the group members, and key generation (key agreement) where all members contribute to a key without this key being transmitted.

For small or stable groups, key agreement protocols are feasible. These are extensions of the Diffie-Hellman algorithm to support more than two peers, as is required for multicast. There are several sophisticated ideas to negotiate a key via multicast messages to minimise the amount of packets. A meaningful approach is the tree-based key generation.

But this raises the question of reliable multicast. However as the group becomes larger the communication complexity grows. Large, dynamic groups require frequent re-keying. Current research therefore focuses on the reduction of costs by switching from key generation to key transport. There are existing drafts already providing meaningful and efficient algorithms and protocols for that purpose.

A service provider first needs to carefully investigate a service’s security requirements, before a meaningful compromise can be found. Because of the costs, a service should offer only those security features that are really needed. If key transport is sufficient, the algorithms, protocols, and standards to implement the service are already available. To develop and offer such a service now, may be the first step into a new market.

2.1.3 Standardisation

In June 2001 the MSEC working group of the IETF published a draft on “Group Key Management Architecture” [11] providing a reference architecture for multicast key management. The intention of this draft has been to put together the concepts discussed so far in the MSEC group and to define a common wording for future standardisation. The MSEC draft covers all types of multicast services. Specifically, the architecture does not restrict the number of senders, nor does it prohibit a group member from being sender and receiver at the same time.
The MSEC draft defines three different tunnels to secure the whole communication:

- **Data Security SA**: Group members exchange data through the *Data Security SA*. The Data Security SA is a unidirectional multicast SA. The *Data Security Protocol* for the SA can be chosen freely. IPSec ESP is mentioned as a prominent example. The key to encrypt the content of the Data Security SA is the so-called *Traffic Encryption Key (TEK)*.

- **Re-Key SA**: The *Re-Key SA* is a unidirectional multicast SA to re-key the Data Security SA. A central component called the *Key Distribution Centre (KDC)* distributes the parameters of the Data Security SA. Typically it also distributes the TEK. Furthermore the Re-Key SA is used to re-key the Re-Key SA itself. The key securing the Re-Key SA is called the *Key Encryption Key (KEK)*.

- **Registration SA**: The *Registration SA* is the only bi-directional unicast SA in the whole architecture. It is the starting point of communication. Group members have to establish an initial Registration SA with the KDC to authenticate and to receive the parameters of the Re-Key SA, especially the KEK. Standard protocols including two-party key negotiation can be used for the Registration SA, e.g. SSL/TLS or IPSec with IKE.

The software component performing the key exchange and managing the Registration SA and the Re-Key SA for the group members and at the KDC is called *Group Key Management (GKM)*.

The architecture minimises the amount of unicast communication to address the requirements of large groups. Each member only needs a single unicast connection to the KDC. Afterwards all information is “exchanged” via multicast tunnels.

As far as possible, standard and well-known protocols can be used. Specifically, the main Registration SA does not require any new protocols. The MSEC draft specifies that according to the needs of a certain service, not all components have to be implemented in all their complexity. Furthermore some details are left to the implementers of a protocol or service.

Currently MSEC works on filling the gaps, i.e. defining the exact content of the Registration SA and the Re-Key SA including the data format. So far, the draft leaves open the issue of *Announcement*, i.e. the method by which possible group members get informed that there is or will be a) a multicast session, b) where to reach the KDC, and c) what requirements (certificate, bandwidth, location, multimedia capability) they need to fulfil to join the session.

The security requirements of multicast services vary a lot. So a generic protocol is needed that can be configured to meet the different requirements. IKE is the protocol for key establishment in unicast IPSec. IKE offers a lot of flexibility for negotiating different types of tunnels. But this flexibility is reached by leaving many parameters and algorithms optional. Therefore IKE has already been criticised as being too
complicated. Furthermore, IKE permits different interpretations, making interoperability the exception, not the rule. This conflict between flexibility and simplicity is one of the reasons why the standardisation process in this area is quite slow and raises a lot of discussions.

The current approach within IETF to create a multicast key establishment protocol by extending IKE or at least copying the basic ideas, would imply the same disadvantages for the new protocol. While there are several discussions to define a simplified version of IKE for unicast, a new multicast protocol is developed that may be even more complicated and error prone. Unless the current drafts are dramatically simplified and clarified, there is a great danger that they will never be implemented!

2.2 Multicast Applications and Services

The following table characterises the services that may benefit from IP multicast, providing some parameters relevant to deciding on a security policy. Certain assumptions, on how the services may be realised, were necessary to fill the table. So a specific implementation may vary in one or more characteristics.

<table>
<thead>
<tr>
<th>Service</th>
<th>Duration</th>
<th>Data Volume</th>
<th>Receivers</th>
<th>Senders</th>
<th>Fluctuation</th>
<th>Exclude Members</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pay-per-view A/V</td>
<td>short</td>
<td>high</td>
<td>many</td>
<td>One</td>
<td>low</td>
<td>no</td>
</tr>
<tr>
<td>Pay-per-month A/V</td>
<td>long</td>
<td>high</td>
<td>many</td>
<td>one</td>
<td>high</td>
<td>no</td>
</tr>
<tr>
<td>Pay-per-minute A/V</td>
<td>long</td>
<td>high</td>
<td>many</td>
<td>one</td>
<td>high</td>
<td>yes</td>
</tr>
<tr>
<td>Push Media</td>
<td>short</td>
<td>low</td>
<td>many</td>
<td>one</td>
<td>low</td>
<td>no</td>
</tr>
<tr>
<td>File Distribution/Caching</td>
<td>short</td>
<td>high</td>
<td>few</td>
<td>one</td>
<td>low</td>
<td>no</td>
</tr>
<tr>
<td>Announcements</td>
<td>long</td>
<td>low</td>
<td>many</td>
<td>one</td>
<td>low</td>
<td>yes</td>
</tr>
<tr>
<td>Monitoring</td>
<td>long</td>
<td>low</td>
<td>few</td>
<td>one</td>
<td>low</td>
<td>yes</td>
</tr>
<tr>
<td>Conferencing</td>
<td>short</td>
<td>high</td>
<td>few</td>
<td>multiple</td>
<td>low</td>
<td>no</td>
</tr>
<tr>
<td>Distance Learning</td>
<td>short</td>
<td>high</td>
<td>average</td>
<td>one</td>
<td>medium</td>
<td>no</td>
</tr>
</tbody>
</table>

**Legend**

- **Duration**: Duration of a session or subscription
- **Volume**: Data volume/sec of the distributed traffic
- **Receivers**: Number of receivers per session or subscription
- **Senders**: Number of senders per session or subscription
- **Fluctuation**: Fluctuation of members
- **Exclude Members**: Necessity for excluding members during the lifetime of the service

The *italic and underlined* entry indicates a parameter value that may make it more difficult to add security features to the service. What the security requirements are (confidentiality, integrity, ..) mainly depends on the content of the multicast session (stock quotes vs. time signal) and on the commercial implications (pay-per-view vs. advertising).

There is a common assessment of the complexity of different services. This assessment is based on the experiences gained with unicast implementations. But this assessment does not hold for multicast implementations. A prominent example is the comparison of a/v streaming and a/v conferencing. In a unicast scenario, large scale streaming raises bandwidth problems, while conferencing is more complicated regarding the security requirements. The bandwidth issue of a/v streaming is solved by multicast, but depending on the service, security may become a major issue.
2.3 Demonstrator

2.3.1 Scenario “Pay-per-month a/v streaming”

Though some standardisation issues are still open, current technologies and protocols already provide the mechanisms to secure most multicast services.

‘Only services with many receivers, high fluctuation, and the need to exclude former members (e.g. pay-per-minute streaming) still require more research before they can be implemented’. The purpose of the demonstrator is to prove this statement.

Therefore the most complicated scenario, that is still regarded as realisable, has been chosen: pay-per-month a/v streaming. The response time of such a service has to be very low, so within the Registration SA all information for connecting to the Data Security SA should already be transmitted. The Service Key of the traditional Pay-TV may be mapped to the KEK, but nowadays the Service Keys of traditional Pay-TV are broken within a few hours or days. So multicast Pay-TV may offer additional security if the KEK is changed frequently, e.g. every hour. The customer can retrieve the current KEK and TEK through the Registration SA after authenticating at the KDC, e.g. by means of a certificate stored on a smart card.

A new KEK can simply be distributed by the KDC through the Re-Key SA, because there is no need to exclude members. At the end of a month only, the KEK has to be transmitted to authenticated members only. Typically, members have to register again, and receive the KEK through the Registration SA.

The demonstrator does not aim at implementing a service. Rather it focuses on testing new protocols. So issues like content management, accounting, network performance, etc. were not investigated. Furthermore, the scenario was simplified to reduce the implementation work:

- The demonstrator is implemented and tested on a single platform (PC/Linux).
- All server components (authentication, key distribution, streaming, and encryption) are running on the same machine.
- Neither a Registration SA nor a Re-Key SA is established between the streaming server and the KDC. Instead, the key is written directly into the SAD of the server. That both protocols are working is proved by the communication between the KDC (server) and the client, so there is no need to reuse this protocol between two components running on the same machine.

To complete the scenario, some boundary conditions have to be set:

- The clients authenticate by means of certificates.
- Audio and video are transmitted in separate streams using a different RTP/UDP port number. But they use the same multicast address and therefore both streams share a single data SA, applying IPSec ESP.

The demonstrator does not address the problem of excluding former members at the end of a month, because these members can only decrypt the traffic as long as they do not disconnect.

2.3.2 Software Design / Implementation Tasks

To avoid re-inventing the wheel, standard implementations already available on the market, are used for most components (LIVE.com and MIM a/v streaming SW, SSH IPSec Express Toolkit (supporting multicast), OpenSSL). Yet, a Re-Key protocol - necessary for this scenario - is not compliant to IETF MSEC. This was solved in the demonstrator by using IPSec ESP. For the content transmitted through this Re-Key SA, a proprietary protocol had to be defined and implemented.

After the main design (see Figure 3) and implementation concept had been agreed upon, the IETF MSEC draft was published (see Section 2.1.3). Fortunately, these basic ideas were quite similar. So only some minor modifications were necessary to make the demonstrator a prototype for an implementation according to the MSEC draft.

1 As in the data security SA
2.3.3 Standardisation Gaps

When designing, specifying, and implementing the demonstrator, several standardisation gaps were identified. Where details or even concepts were not yet standardised, reasonable decisions had to be made. But as long as these issues are not addressed by MSEC, the solutions will be proprietary and not interoperable. The future will show if the attempt to forecast the results of the standardisation bodies has been successful or not.

- **Reliable Re-Keying:** An open issue of secure multicast, currently discussed by the standardisation bodies, is related to the non-reliability of IP multicast. A group member who does not receive the new key, will be excluded until the key is distributed the next time, or the group member may have to register again. Current solutions are based on the prophylactic retransmission of keys.

- **Key Selection during Registration:** In contrast to unicast tunnels, multicast tunnels typically are already in use when a new member joins the group. So the lifetime of the current SA may be just about to expire. The KDC needs to decide what key to provide to a new member during registration. If the current key is sent, it may already have expired when the new member receives the first traffic. If the next key is sent, it may take some time until the new member can decrypt incoming packets.

- **SA Synchronisation:** Before a new Data Security SA, with a new key, takes the place of the previous one, the new key has to be distributed. But distributing the new key is done by the KDC, while switching to the new SA is done by the senders of the group. A mechanism is missing which indicates to the senders that the key distribution is complete and that the new key should be used immediately. On the one hand, it should be the KDC to decide when a new key has to be activated and not a group member, even if it is the only sender. On the other hand, a sender should not rely on the key distribution to work properly, because in this case a single member could block re-keying infinitely, by simply signalling that it failed to receive the new key.

- **Member Exclusion:** At least in the pay-per-minute scenario, former members need to be excluded from the list of receivers. Therefore the TEK has to be changed. To keep the former member from receiving the new TEK, the KEK has to be changed, too. To keep the former member from receiving the new KEK, the KEK has to be distributed in a confidential way. There are only two solutions to this problem: either each member uses a separate unicast tunnel to retrieve the new KEK, or the whole Re-Key Protocol switches from key transport to key generation. This topic is discussed in more detail in Section 2.1.2.
• **Member Termination:** The IP multicast protocols include mechanisms to detect if group members are no longer listening to a multicast address. But these mechanisms are transparent to the sending application. For some types of multicast services, it is necessary to know what receivers are listening to a certain address and when; especially for accounting purposes. The pay-per-minute scenario is an example. A service should offer the means to a member to quit explicitly. Nevertheless, quitting also has to be detected automatically, e.g. in the case of software, network, or power failure. Therefore the members need to send some kind of ‘keep-alive’. Apart from the additional traffic, the ‘keep-alive’ raises some security problems.

• **Compatibility with ISAKMP:** Although the Registration SA is two party, unicast, and bi-directional, and the Re-Key SA is multiparty, multicast, and typically unidirectional, there is quite an overlap between both SAs regarding their content. The Registration SA as well as the Re-Key SA have similarities to the ISAKMP/IKE SA of standard (unicast) IPSec. So it is likely the IKE protocol and data format will be adopted. To extend an existing protocol is a valid approach, but the derived version of IKE may become even more complicated than IKE itself.

• **Sequence Numbers and Multiple Senders:** ESP and AH use sequence numbers for an anti-replay service and possibly for loss detection. If multiple senders are present in a multicast group, the sequence numbers they use cannot be synchronised. Therefore the receivers need to keep track of the different sequence numbers of each sender separately, though they all use the same SPI, security protocol, and keys.
3 IPVPN Components and Remote Users

3.1 Technical Issues Related to Remote Access

To connect a remote access user via a 3rd party IP network by means of VPN, two methods are known nowadays:

**Compulsory Tunnelling** (Figure 4) uses the L2TP-protocol to establish a VPN-tunnel between the dial-in server/LAC (*L2TP Access Concentrator*) and the corporate network’s gateway/LNS (*L2TP Network Server*). Call routing for compulsory tunnels requires that some aspect of the initial PPP call set-up can be used to allow the LAC to determine the identity of the LNS, according to [10].

![Figure 4 Compulsory Tunnelling example](image)

**Voluntary tunnelling** (Figure 5) can be supported by the L2TP specification, insofar as the LAC can be located on a host, not only on a network node. Such a host has two IP addresses - one for the LAC-LNS IP tunnel, and another, typically allocated via PPP, for the network to which the host is connecting. The existing authentication and address assignment mechanisms used by PPP can be reused without modification. If IPSec is used for voluntary tunnelling, the functions of user authentication and host configuration, achieved by means of PPP when using L2TP, still need to be carried out. The methods of supporting legacy user authentication and host configuration capabilities in a remote access environment are currently being discussed in the IPSec working group.

![Figure 5 Voluntary Tunnelling example](image)
3.2 Smart Card based Remote Access

This section is dedicated to the possible integration of a smart card as a security support for VPN security. This integration provides the following advantageous features: authenticating human beings, independence of the computer, separation of the Private Key and computer and provision of security for many applications involving not only VPN, but also web signing, e-mail, etc.

![Diagram of Smart Card Integration for IPVPN](image)

Figure 6 Architecture of Smart Card Integration for IPVPN

Strong user authentication, by means of keys and certificates stored on his/her personal token (smart card), is assumed for high level security. The standardised PKCS#11 APIs are required between the IPSec client and the driver of the smart card, so as to enable standard replacement of smart card packages. Interoperability of VPNs requires the implementation of the IKE protocol for key exchange. With IKE there are four authentication methods which are possible:

- Authentication with digital signatures,
- Authentication with public key encryption,
- Authentication with a revised mode of public key encryption,
- Authentication with a pre-shared key.

The security should rely on the deployment of a Public Key Architecture. The certificate stored in the personal token of the client is signed by the private key of the Certification Authority (CA). The public key of this CA is available from a server, or from the gateway on the VPN end point.

The use of smart cards adds an aspect that shall be carefully considered when it comes to the difference between user level authentication and machine level authentication.

A Telco can sell a VPN service secured by its own CA, issuing certificates that are installed in Provider Edge equipment. These certificates are used to establish IPSec SAs. The CA issuing the certificates is the Telco CA. If the corporate has its own CA for the support of the security services inside its domain, the two levels
of authentication can be separated. The VPN security guaranteed by the Telco relies on the Telco certificates and ends up at the LAN gateway, whereas end-to-end security is assumed by the corporate application and relies on the corporate certificates.

Figure 7 Multiple PKIs

When a smart card is used, different scenarios may come up:

1. If the IPSec protection ends up at the SG, the user personal token (smart card) may contain only the user application-level certificate issued by the corporate CA; the Telco certificate is installed in a part of the Provider Edge equipment or the secure gateway;

2. If the IPSec protection goes end-to-end, there is a possibility that the user personal token will contain both the Telco-issued certificate and Corporate-issued certificate, stored in different files of the smart card.

3. Eventually, in the case of end-to-end IPSec protection, a unique certificate (either issued by the Telco or the corporate) can be used for both application-level security and IP level security. In this case we resume to Scenario A.

The global integrated application is complex and very few actors in the network industry provide such a product:

- The VPN IPSec is included in the third layer of the OSI model, at the border between layer 2 and layer 3. This could result in an integration conflict with a possible ADSL module. In this profile, some upper layer application could also use some cryptographic module such the smart card pack and could create a second difficulty resolved by a multi-thread application for the API of the smart card.

- In this profile, some upper layer application could also use some cryptographic module such the smart card pack and could create a second difficulty resolved by a multi-thread application for the API of the smart card.

- Another difficulty addresses specifically the network layer in the interoperability aspect of all the IPSec implementations to each other and in particular the problems caused by the key management of the options of the protocol IKE or any of the other protocols such as GSS-API, that are not compatible with IKE.

- Another potential problem concerns the smart card part: For example, some VPN module has a specific API or does not have the same version of a standard API. Two major APIs (PKCS#11 and CAPI) can interconnect the smart card reader and the VPN integration. But in both cases, the pool of functions included in a version of the standard must be the same on each side of the API.
Finally, the VPN must be completed by a distributed firewall in the role of protecting the remote system from viruses or Trojan Horses installed before and able to open ports on the Internet during an intranet connection.

3.3 PKI applied to Remote User Scenarios

This part briefly describes the use of a PKI (Public Key Infrastructure) for security of communication, involving establishment of IPSec Security Associations (SAs), between the resources of an enterprise and employees remotely connected, in various scenarios.

The PKI is in charge of distributing certificates so as to enable the different entities of a VPN to further establish secure channels between themselves. A SA is a relationship between two or more entities, defining in which manner these entities utilise security services to protect their communication.

Scenario 1 (Remote Individual)

A small/medium enterprise PKI with a unique CA; a mobile employee connects through the public network.

![Figure 8 Small/medium enterprise PKI](image)

There is a need for a security association between a laptop remotely accessing a server located on a corporate LAN, on behalf of a mobile employee of the enterprise. It is assumed that an IPSec SA may be established, from the employee laptop to the corporate gateway, or to the required resource, or both. An authorisation server is assumed within the corporate LAN in order to allocate resources to the assessors in line with their privileges in the enterprise.

Scenario 2 (Satellite Office)

A small/medium enterprise PKI with a unique CA may include satellite office/home office. In this scenario, the enterprise workforce is remote, but not necessarily mobile. The PKI applicability is the same.

Scenario 3 (Roaming Employee)

This scenario addresses the needs of large enterprises to set up secure connections with remote branches, retailers, or subsidiaries.
The mobile user in the remote branch premises holds a certificate, from the authorisation server in the branch office LAN, signed by a CA, that is not directly known.

The visitor has two main options:
- Connection through a modem via the public network.
- Connection to the branch office LAN in order to utilise a better bandwidth.

The following SAs are needed:
- One SA between the visitor and the (blue, lower) authorisation server for visitor authentication and granting minimum access rights in the visited LAN;
- One SA between corporate gateways to establish a secure tunnel between corporate LANs;
- One SA between the visitor and his home application in order to establish a secure communication between the visitor and the required resource in his home LAN.

Implied requirements for PKIs:
CA1 publishes a certificate with CA2 public key signed by CA1 private key; simultaneously, CA2 publishes a certificate with CA1 public key signed by CA2 private key. The verifier in the CA2 domain should additionally check the status of the visitor's certificate. This implies that it can retrieve the CRL related to CA1. This is a problem in existing implementations that generally do not support all the complex features necessary for CRL verification along a chain of certificates.

This could be done by deferring the complete process to a server dedicated to certificate validation (SCVP: Simple Certificate Validation Protocol).

### 3.4 Usage of PKI to Automatically Initialise IPSec

The use of public key certificates has to be managed. This management has to cover the whole life cycle of the certificate from enrolment to revocation. To reach this objective, different proposals have been made by the IETF. Two of them are described below: SCEP and CMP.
3.4.1 CMP protocol description

CMP (Certificate Management Protocol) is an IETF standard (RFC 2510) which specifies the functions that must be implemented in a PKI.

Three entities are defined: End Entity (EE), Certification Authority (CA) and an optional Registration Authority (RA). These entities shall have "Secure local access" to sensitive information such as the private key, the public key, and the trusted CA public key.

The CMP mechanism specifies that the CA provides, out-of-band, an Initial Authentication Key to the EE. This key is used to protect the messages exchanged during the certificate request. Then the EE generates a pair of keys and creates a message for the certificate request and sends a message request protected with the Initial Authentication Key. The CA will process the request, or not, depending on the result of the above message authentication. If the request is in conformance with its policy, the CA sends a signed certificate to EE. The EE sends a message confirming that it has received the certificate. The CA verifies the authentication of the confirmation message. If the confirmation is not authentic the CA revokes the certificate.

3.4.2 SCEP Protocol Description

The SCEP protocol, designed by Cisco, was submitted to the IETF as an Informational Draft. It specifies the communication between an "End Entity" (EE) and a PKI for certificate enrolment and revocation.

Two entities are relevant in SCEP; the "End Entity" and the CA (CA and RA are referred to as the same entity). The EE takes the initiative for all the messages. In the IPSec VPN context an EE is either an "IPSec Client" or an "IPSec gateway". SCEP does not mandate the EE to have enough memory to store its own certificate. This means that the CA should save all the certificates that it issues.

During the initialisation process, SCEP uses the self-signed certificate principal during the certificate request. This technique does not authenticate the signer, but it permits the establishment of a secure channel between the peers during the enrolment phase. When the CA receives the certificate request, it has to authenticate the identity claimed in conformance with its policy.

3.4.3 Comparison between the Protocols

<table>
<thead>
<tr>
<th>Table 2 Comparisons between SCEP and CMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entities</td>
</tr>
<tr>
<td>EE, RA, CA</td>
</tr>
<tr>
<td>Certificate enrolment</td>
</tr>
<tr>
<td>Revocation request</td>
</tr>
<tr>
<td>Update Request</td>
</tr>
</tbody>
</table>

EDIN 0300-1107 © 2002 Eurescom Participants in Project P1107
3.5 Remote Users via Mobile IP

3.5.1 EURESCOM P912

In EURESCOM Project P912 [15], security considerations for IP-mobility have already been studied. The focus was mainly on radio access networks connected by the internet. No domain boundaries to segregate different administrative, addressing/routing or security policies were investigated. Instead, different dynamic scenarios were investigated, where the involved user moves between different access networks.

However, this project (1107) investigates what security requirements have to be taken into account, if mobile users are static but can visit different places with different network properties and can communicate with correspondents residing in different networks with different network properties. The common element is the need for participating in a secure communication environment.

3.5.2 VPN-Scenarios for the MIP User

Many opportunities exist to create VPNs, but the architecture always depends on the concrete communication scenario.

The Peer-to-peer VPN scenario for roaming users (Internet) assumes that two roaming instances residing in the Internet want to communicate with each other and that these two instances have pure Internet access only (they do not create a VPN tunnel to an associated Intranet).

This scenario, illustrated in the diagram below, is characterised by assumptions that communication should be secure and the Mobile Node has a public IP address. PPP is used to access the Internet and the ‘Care-Of’ Address will be assigned dynamically per DHCP (no Foreign Agent). The Co-located Care-Of Address is routable within the Internet domain to which the Home Agent and POP belong.

The Campus network (Intranet) scenario consists of a local network operated by a single provider isolated from the Internet. Usually a campus network is separated into a number of IP sub-networks reflecting the organisational structure of the campus. There are no firewalls within the campus network, separating different departments and IP roaming is the solution for mobility.

---

2 “static” here means that they do not move for at least a number of minutes.
The Intranet remote access via MIP (Internet-Intranet) scenario presented in the following picture, assumes that the Intranet (Network A) is segregated from the Internet (Network C) by a firewall, and a Foreign Agent is demanded in the access network of the Internet.

![Network configuration Internet-Intranet](image)

**Figure 12 Network configuration Internet-Intranet**

The Intranet remote access via MIP (Intranet-Intranet) scenario supposes that a Mobile Node moves to a private Network B, which is assumed not to be managed by the same administration at its home network. Both networks are similarly structured and are separated by the Internet (Network C).

![Network configuration Intranet – Intranet](image)

**Figure 13 Network configuration Intranet – Intranet**

### 3.5.3 Overall Security Requirements and Countermeasures

In all the scenarios, the protection of data can be accomplished in two steps: Integrity protection of Data through IPSec and AH, and Integrity protection and the Confidentiality of Data through IPSec and ESP.

- **Internet:** For protection of the Mobile IP utilisation in the Internet, the following overall requirements have been derived:

  **Procedure for Registration:** The affected endpoints are Mobile Node and Home Agent. The only security measures necessary are for the prevention of tampering and forgery of the contents of the IP packets and the guarantee of their confidentiality. An Encryption method between the endpoints Mobile Node and Home Agent, as well as over the segments between Mobile Node-Foreign Agent and Foreign Agent-Home Agent will, for the moment, be considered to be equivalent. One possible method would be IPSec and ESP.

  **Data traffic:** Data traffic is sent between the two endpoints Mobile Node and Correspondent Node, although different paths are taken for each direction. With a protection solution providing End-to-End coverage, this is of no importance.

- **Campus network (Intranet):** The same protection measures discussed in the Internet scenario are needed.

- **Intranet – Internet:** Some of the Transmission Segments are protected by the FW, and others are unprotected in the Internet. In order to keep the security level of the entire concept uniform, it is
imperative that the segments in the Internet are also protected through certain security measures. Derivations of the Internet scenario security solutions are used.

- **Intranet – Intranet**: All Nodes, including the Correspondent Node (Correspondent Node 1), are to be found within a part of the Network that is behind the firewalls and the Correspondent Node (Correspondent Node 2) is the only Mobile IP component to be found outside both FW protected Networks.

### 3.5.4 Security Solutions per Scenario

To avert the threats described in the previous section, IPSec generally provides all functionalities needed. When combining both protocols (MIP and IPSec), some non-trivial problems arise. We may find a proper solution to these problems for each scenario, but the creation of an overall scenario will be very complex and does not seem to be realistic.

**Peer-to-peer VPN (Internet)**: Only two security associations are established. Because there is no sensitive data exchanged during the registration process and the integrity of the registration data is assured through Mobile IP, no reference to the establishment of further IPSec Security Associations (i.e. between MN and HA) will be made at this point.

**Campus network (Intranet)**: If it is a closed network where each member node is considered as “trusted”, there is no need for security. If the trustworthiness of the nodes is questionable, the threat analysis is very similar to that of the Internet scenario.

**Internet – Intranet**: Under the predetermined circumstances of NAPT in the FW-system, the home network of all MNs is selected to be the DMZ of the Intranet. Therefore, the subnets of the Intranet must make FA functionality possible, if a fixed address scheme is applied.
When deciding on the location of an IPSec gateway, the disadvantage of a restricted Mobile IP (by the combination of the FA with the MN) is more important than the disadvantage that comes from having the HA in the DMZ. Therefore, the following topology was designed with the assumption of the HA being the IPSec gateway in the DMZ.

When considering the location of an IPSec gateway, the disadvantage of a restricted Mobile IP (by the combination of the FA with the MN) is more important than the disadvantage that comes from having the HA in the DMZ. Therefore, the following topology was designed with the assumption of the HA being the IPSec gateway in the DMZ.

**Figure 15** Network distribution outline of Mobile IP functions after setting up a DMZ

---

### Intranet – Intranet

The firewalls function also as IPSec gateways. Contrary to the implementation in the requirements catalogue, the CN’s that are positioned outside the Intranet in the Internet will not be taken into consideration here. Therefore, this implementation leads back to the Internet - Intranet scenario.

---

**Figure 16** Resulting protocol encapsulation for Intranet–Internet scenario

---

3.5.5 Conclusion

In order to create an overall technical solution for the four scenarios, a number of problems arise. Nevertheless, in general, MIP based IP-VPNs can be realised. This provides the opportunity for compatibility with 3G all-IP networks (and 4G) from the beginning.
4 Inter-working of Security Technologies

4.1 Security in VPN Architectures

4.1.1 Risks and Security Requirements

The use of VPNs raises several security concerns beyond those present in traditional corporate networks. In a heterogeneous environment, there are many opportunities to eavesdrop, to read and change a datagram’s content, to mount denial-of-service attacks, or to insert external packets in the traffic of the VPN. If the VPN traffic traverses networks or equipment owned by multiple VPN providers then strong security mechanisms may be appropriate. Also a strong level of security may be applied by a provider to customer traffic to address the customer perception that networks, and particularly the Internet, are insecure.

According to [9] seven security requirements for VPN implementations are identified:

- Address Separation
- Routing Separation
- Traffic separation
- Core structure hiding
- Data confidentiality, integrity and authentication
- Traffic flow security

4.1.2 Risks and Vulnerabilities for Different VPN Models

Applying the security requirements identified in the previous section to link layer-based VPNs like ATM, FR and X.25 as well as to overlay-based VPNs like GRE, IPSec and L2-tunnel protocols should eliminate the known vulnerabilities and prevent potential attacks.

- **Frame Relay, ATM, X.25:** Address, L3-routing and traffic separation is not an issue, since the provider backbone is layer 2. Core structure hiding is handled quit well since the only information exchanged between the service provider and the client concerns data rates and L2 labels like Frame Relay DLCIs or ATM VPis/VCl which have a local relevance only. Spoofing, sniffing, replay, session hijacking, DoS and man-in-the-middle attacks are not feasible from the outside of the network, however these kind of VPNs are vulnerable from inside the core network.

- **GRE, IPSec, L2TP, L2F, PPTP:** Addresses on the customer site are hidden from the core network. The core network terminates IP-tunnels and runs potentially insecure routing protocols interfacing all customer routers no matter what VPN they belong to. In addition the customer may have access to the core network’s common address space. A clear address segregation must prevent access to VPN address space from the core network’s address space. Regarding traffic separation, it should be possible to inject data towards other customers VPNs since all traffic is forwarded on the same logical entities. Since the termination of IP-tunnels is done within the global core L3 address space, it isn’t easy to hide the core details from the customers.

Resistance to Attacks: If the routing protocols being used have security weak spots, signalling attacks can be performed and traffic deviation could be possible. As IPSec provides data confidentiality and packet level authentication, it is resistant to Replay and Session Hijacking attacks.

- **Virtual Routers (VR):** Virtual routers provide the same functionality as physical routers but within one box. While the resources of the device are logically separated, a VR can share common network resources, where the traffic between two VR-instances is identified by a designated VPN-ID. Different levels of data, routing and configuration security can be implemented. Existing security mechanisms such as password, RADIUS, etc. can be available to the VPN user.

- **MPLS:** Comparable to ATM and FR, MPLS-VPN enforces traffic separation between customers by assigning a unique VRF (Virtual Routing and Forwarding table) to each customer’s VPN. Traffic separation occurs without tunnelling or encryption because it is built directly into the network itself. MPLS doesn’t reveal additional unnecessary information even to customer VPNs. Static routing can be configured between the PE and CE. By these means the MPLS core can be kept completely hidden and be addressed using a public or even private address. It is possible to attack the MPLS core and to attack other VPNs from there by attacking the PE routers directly and by attacking the signalling mechanisms
of MPLS. Deliberate or inadvertent miss-configurations from SP staff may result in undesired behaviour including severe security leaks.

### 4.1.3 Countermeasures

- **Packet filtering**: A packet filter is a piece of software that looks at the header of packets as they pass through, and decides whether to DROP or ACCEPT the packet.

- **Address hiding**: IPSec provides a means to hide private or internal IP addresses. In IPSec tunnel mode, all the tunnelled traffic, including IP headers are hidden from external observers.

- **Routing Protocol Security** (e.g., BGP/MD5): Historically, routing protocols used within the Internet have lacked strong authentication mechanisms. Recently, cryptographic authentication mechanisms have been developed for RIPv2, OSPF, and the proprietary EIGRP routing protocols.

- **Route filtering**: Route filtering has been found to be a particularly effective method to stabilise Internet routing. It has long been recognised that prefix-based filtering must be used at strategic points in order to prevent bad routes from being injected into the global Internet.

- **Route dampening**: keeps routes that are flapping (because there are a big number of connection announcements in the net) from consuming significant network bandwidth.

### 4.2 MPLS-based VPNs and IPSec Inter-working Scenarios

This scenario set includes IPSec on the remote access to the VPN, across the provider network, between the final communication entities (end-to-end) and between two provider networks.

#### 4.2.1 Secure Remote Access (CE-PE-Scenario)

The most common secure CE-PE scenarios are where the host computer performs voluntary tunnelling with IPSec or the host computer is running IPSec to secure a PPP/L2TP session. All the standard IPSec features for authentication and encryption can be used without modification in CE-PE scenarios.

Besides the scalability problems, IPSec causes some problems if there is a need for legacy authentication systems (e.g. RADIUS). Currently defined authentication mechanisms for IPSec are symmetric, or both sides authenticate using identical public key mechanisms (encryption or signatures). For most remote access scenarios, the IP address of the remote user simply is not known *a priori* and/or one time pass phrase mechanisms are used.

Legacy mechanisms typically provide one-sided authentication for the user but IPSec does not. Hence, in order to support legacy authentication mechanisms within IPSec, it must either be possible to authenticate the user and the gateway asymmetrically, or it must be possible to derive a user credential from the legacy authentication process which may then be used to secure an IPSec connection.

There are a number of proposed solutions for the problems described above. However, they do so in several different ways. The techniques fall into 3 general categories:

1. Those which complete IPSec negotiation (phase 1 and/or phase 2 IKE) prior to authenticating the user:
   - XAUTH/MODECFG - XAUTH refers to eXtended AUTHentication (within IKE).
   - HYBRID – built on the XAUTH/MODECFG combination, adds one-sided server authentication.
   - L2TP - L2TP (Layer 2 Tunnelling Protocol) uses PPP-based authentication.

2. Those which integrate the user authentication into IKE phase 1 negotiation:
   - CRACK - CRACK stands for Challenge/Response for Authenticated Cryptographic Keys, which integrates the user authentication into IKE phase 1 negotiation.

---

3 These IPSec tunnels may be terminated at a separate VPN-concentrator/IPSec-gateway directly attached to the PE. Alternatively the PE itself might support IPSec/MPLS-inter-working.
3. Those which move the user interaction outside of IPSec entirely:
   - PIC - PIC stands for Pre-IKE Credential provisioning protocol, (discussed in [12]) and GetCert - GetCert is a shorthand name for “Client Certificate and Key Retrieval for IKE.

All of the proposed mechanisms solve the most basic problem, which is to authenticate remote access users by way of legacy authentication systems (e.g. RADIUS). Although, the only proposals which meet all the requirements are GetCert and PIC (when implemented on an outboard authentication server).

4.2.2 IPSec Tunnels Across SP Networks

The scenario shown in the figure below assumes that the IP traffic between the PEs of a service provider VPN network has to be encrypted and authenticated with IPSec.

A VPN customer could use the security services of the VPN service provider to encrypt and authenticate his traffic between different sites without implementing IPSec in his routers or hosts. The security policies, which should by applied to the traffic between different customer sites, could be defined by the customer himself, the service provider or by both together. The design and specification of a security policy assumes a certain minimum amount of expertise in cryptography, IT security and network protocols.

If the VPN customer has experience in specifying a security police it may also be possible, that the service provider offers an interface, such that the VPN customer can maintain his own security policy in a secure manner.

There are several approaches discussed on the topic of specification, management and distribution of policies in IP networks:
   - The IPSec Configuration Policy [13] attempts to describe the policy aspects of IPSec in an abstract, conceptual and object-oriented manner.
   - The IPSec Policy Information Base [14] consists of a series of tables that contain policy-related information. The tables are delivered to IPSec hosts or gateways from a policy server.

Incoming IP packets from the customer at the ingress PE should be secured from a security gateway (SG) applying an IPSec-tunnel. The SG is directly bound to the PE and may be an integrated software module or a separate device. In the case of multiple VPNs/customers connected to one PE, the assigned SG can be shared between them. To provide a type of traffic separation, all SPIs of a VPN should be in a fixed range. We assume that the MPLS routes are static and the inbound SG knows the IP address of the corresponding outbound SG with respect to a customer’s IP packet. This can be done by centralising route and SG configuration and management.

The derivation of symmetric keys used for encryption and authentication is not addressed here and delegated to IKE.
Between PEs, IPSec-rules are applied to all traffic. The security gateways ensure that all customers’ traffic across the network is protected by IPSec in tunnel mode. Denial of service attacks is not possible, since only traffic from the VPN customers can reach the security gateways and the provider routers.

Due to the use of BGP in MPLS networks, routing information from the customer must not be protected by the security gateways.

The most common and practical scenario would be, that the MPLS routers (PE) are capable of IPSec. In this case it should be possible that the IPSec module is aware of the outbound SG with respect to an IP packet. Also, in the first phase of the implementation of a PE-PE scenario, pre-shared secret keys between the SGs of the SP should be used to protect the IKE exchanges. In the second phase, a PKI should be established for the SPs network.

4.2.3 End-to-End IPSec Tunnels

In the context of this document end-to-end IPSec tunnels are established between customer sites across an existing VPN. The difference to the PE-to-PE IPSec tunnels described above is, that the security gateways (SG) are moved to the customer sites. Therefore end-to-end tunnels are also called CE-to-CE tunnels.

From the protocol point of view nothing changes when the security gateways reside at the customer site instead of on the SP’s side. But from the management or marketing point of view, there are significant differences: Configuration is less complex - since every SG serves only one VPN – but, for the same reason, hardware and administration costs are very high for the customer.

The packets passed over the link between the CE and the PE are already encrypted and in that way protected against eavesdropping. The customer does not necessarily need to trust all the SPs involved in the VPN. Possible exchange of routing information as described in the previous section does not have to be taken into account by the SP. Every site belonging to an IPSec VPN only uses a single IP address, related to the corresponding IPSec tunnel.

IPSec hides upper layer information from the underlying backbone. This is a security feature, but it raises problems, if the backbone needs to evaluate information like IP addresses or port numbers, e.g. for assigning QoS.
4.2.4 IPSec Tunnels Between SP Networks

IPSec tunnelling can also be used to connect PE routers of different SP networks over a public network, e.g. the Internet. This might build extranets between VPN customers, which are connected to different SP networks but it is essential for the IP traffic running over the public network to be encrypted and authenticated in order to reach the same security level as within an SP network.

The PE to PE scenario with two SP networks is shown in the following picture. The two SPs use security gateways to connect their networks with an IPSec tunnel via the public network.

![Figure 20 IPSec tunnels between SP networks](image_url)

The service providers should encrypt and authenticate all IP packets regardless of their content and their source and destination addresses. This should explicitly include the exchange of routing information between the two PEs. On the security gateway, one instance of IPSec will be used with exactly one SPD securing exactly one connection per PE-PE connection.

The symmetric keys for the IPSec encryption and authentication will be derived by the IKE protocol. For the authentication of the IKE messages, either pre-shared secrets (which have to be exchanged out-of-band between the service providers) or PK certificates may be used.

Protection of customer traffic and routing information can be performed by the rigorous encryption of all IP traffic going over the public network. To prevent introduction of 3rd party IP traffic, the IKE messages exchanged between the security gateways must be authenticated either by using pre-shared secrets which are different for each SG or by PK certificates for the SGs. The use of one pre-shared secret which is the same for all SGs is not sufficient since then it is not detectable what SG was the originator of the corresponding security association.

4.3 Test and Demonstration

4.3.1 Testbed Implementation

This section aims at testing the previously described VPNs’ security requirements in a pure MPLS and in a combined MPLS / IPSec VPN from two perspectives:

- Outside / Customer perspective attacks - OPA
- Inside / Core perspective attacks - IPA
4.3.2 Tests Definition

1. **Address and Routing Separation – OPA:** Two different VPNs with the same address range are used. It should be verified that the CE, PE and P routers have consistent forwarding information in order to prove that routing separation exists.

2. **Traffic Separation – OPA:** Tests if traffic injected in one VPN stays in that VPN.

3. **Core Hiding – OPA:** In MPLS networks, core routers’ network addresses are not known to the customer. The only information the customer needs to have is the connected PE interface IP address. The exchanged BGP information should only reflect client networks from the same VPN. This test will be done knowing the internal IP addresses and sending ICMP traffic from the client LAN to the PE and P routers core interfaces.

4. **Routing DoS attack – OPA:** This test assesses the effect of injecting routing messages at high speed from the CE router against the PE customer interface. These attack tests should be divided in two parts: correct messages at high sending rates and wrong routing information messages. The impact on neighbouring traffic should be measured as well as the content of neighbouring CE’s routing messages. Two different scenarios should be considered: with routing filtering and without it.

5. **MPLS label spoofing attack – OPA and IPA:** PE immunity against outside (CE) labelled packets together with P and PE immunity against inside label spoofing should be tested. In order to perform this kind of test, injection tools must be used.

6. **Performance test, if SG is integrated in the PE router:** In this configuration it is investigated if the PE router is sufficiently powerful.

7. **SG between CE and PE router, routing information:** To test if the routing information from the customer’s network is transmitted correctly to the PE router, an IPSec security gateway has to be set up such that the routing information is left unencrypted but all other traffic is encrypted. The test can be performed outside an MPLS testbed but also in the testbed between the CE and PE router.

8. **SG before the CE router, TOS byte:** To provide QoS on the MPLS platform a TOS byte has to be set before the IP packet is encapsulated by the IPSec gateway. The IPSec standard [rfc2401] requires that
the TOS field is copied from the inner IP header to the IP header for the tunnel mode. In this test it will be checked with different IPSec implementations that this setting actually takes place. The test will be performed outside the MPLS testbed with two security gateways and protocol analyser software.

9. **SG before the CE router, routing information:** An IPSec gateway is attached to the CE router. It will be tested if the routing information is transmitted correctly between the CE router and the PE router.

### 4.3.3 Test Results and Recommendations

The detailed test descriptions and results can be found in [4].

The test results have demonstrated that MPLS-based VPN networks have nearly reached the security features of a layer 2 based VPN (Frame-Relay or ATM). Business customers could question the MPLS-VPN networks security but they perform the same features like *Address Space, Routing and Traffic Separation*. Regarding core hiding, by default, Cisco MPLS implementation leaves the core structure visible. Additional configuration is needed to hide it, by means of disabling MPLS TTL or disabling ICMP messages at the “TTL expired” event. Due to enhanced MPLS forwarding mechanisms and routing separation, injecting a high number of forged routing messages in the PE in an attempt to perform a DoS attack, does not affect the forwarding performance of the neighbouring (same PE) VPN networks.

IPSec can be run near or on the PE routers or near or on the CE routers. If the VPN service provider controls the CEs as part of the service, the customer has to decide whether to trust the SP to configure IPSec for him, or whether to maintain control over IPSec in additional equipment outside the SP’s scope. Since PE routers with IPSec could be bottlenecks during high traffic load and the customer wants to control the IPSec configuration in most cases, IPSec should be applied on the CE or behind. For the IPSec tunnels, different topologies are possible: Point-to-point, Hub and spoke or a full mesh. Full mesh would be the most preferable, but is extremely complex to deploy with static configurations, because the total number of peering relations becomes quickly too large to manage.

With IPSec in MPLS-based VPNs and in general, some further problems are introduced: The NAT problem; application of quality of service mechanisms in the MPLS network; and the fast detection of loops on the route of an IP packet. RFC 2401 specifies, that the value of the TOS byte of the original header has to be copied into the new header while applying IPSec. Otherwise QoS mechanisms in the MPLS network may not work correctly. All tested routers show that they can be configured so that they conform to RFC 2401. Not all tested IPSec gateways conform to the standard with respect to the handling of the TTL field. Today, IPSec is the most secure, best supported and flexible technology to fulfil the requirements of data confidentiality, integrity, authentication and replay detection within a VPN. The IPSec and the MPLS technologies can be very satisfactorily combined to build secure and well-manageable VPNs from the point of view of the customer and service provider.
5 Conclusion

Three different aspects of IP-VPNs were explored in this project report:

1. **Key management for IP multicast scenarios;**

   For multicast, many different usage scenarios with different requirements on the supporting network were identified. The most complicated scenario, that is still regarded as realisable, has been chosen for the implementation of a demonstrator: pay-per-month a/v streaming.

   In order to manage the subscription and un-subscription of a large number of clients, a special key management system must be established, that is not covered by the well-known IP specifications. In this project a group key management architecture was specified and implemented successfully. This architecture is now in line with the official IETF architecture proposal [11], [16].

   Despite the successful implementation there are still a number of unsolved problems such as reliable re-keying, SA synchronisation and member exclusion in scenarios with a short-term member verification (e.g. pay-per-minute) or compatibility with ISAKMP.

2. **Remote access and seamless mobile access via 3rd party ISPs;**

   To include remote users via a third party ISP, concepts for a smart card-based user authentication and a suitable PKI architecture were introduced. Since in such an environment more than one trusted instance is needed to establish an end-to-end VPN path, the concepts reflect the arrangement and interactions between different certification authorities that may belong to different administrative domains. It is suggested that authentication and authorisation be certificate based. Certificates can be sent in-band or out-of-band on the designated IP VPN path. Two different protocols representing respectively an in-band and out-of-band solution for an automatic initialisation of IPSec, were also evaluated and compared.

   To seamlessly connect remote and moving users to their corporate networks, the combination of Mobile IP and IPSec was analysed with respect to a detailed threat analysis. Similar to a multicast environment, a number of different usage scenarios with different requirements to the supporting network exist. Here four different scenarios were analysed and according to the threat analysis, concepts for their realisation were proposed. As a result there is no overall architecture that satisfied all requirements. Compromises have to be considered in order to get an acceptable solution. This provides the opportunity for compatibility with 3G all-IP networks (and 4G) from the beginning.

3. **MPLS/IPSec inter-working**

   The results of the MPLS/IPSec inter-working tests have demonstrated that MPLS-based VPN networks have nearly reached the security features of a layer 2 based VPN. Indeed MPLS-VPN security performs the same features as Address Space, Routing and Traffic Separation.

   Given the facts that Provider Edge routers with IPSec could be bottlenecks during high traffic load and that in most cases the customer wants to control the IPSec configuration, IPSec should be applied on the Customer Edge or behind. For the IPSec tunnels, different topologies are possible: Point-to-point, Hub and spoke or full mesh. Full mesh would be the most preferable topology, but is extremely complex to deploy with static configurations, because the total number of peering relations quickly becomes too large to manage.

   With IPSec in MPLS-based VPNs and in general, some further problems are introduced: the NAT issues; the application of quality of service mechanisms in the MPLS network; and the fast detection of loops on the route of an IP packet. All tested routers show that they could be configured so that they are compliant to RFC 2401. Not all tested IPSec gateways are compliant to the standard with respect to the handling of the TTL field.

   Today, IPSec is the most secure, flexible and best supported technology to fulfil the requirements of data confidentiality, integrity, authentication and replay detection within a VPN. The IPSec and the MPLS technologies can be very satisfactorily combined to build secure and good manageable VPNs from the point of view of the customer and service provider.
References


