

HELSINKI UNIVERSITY OF TECHNOLOGY  
Department of Computer Science  
Telecommunications Software and Multimedia Laboratory

**Kari Klemetti**

# **Authentication in Extranets**

Master's Thesis submitted in partial fulfilment of the requirements for the degree of  
Master of Science in Technology.

Espoo, 25th July 2001

Supervisor: Professor Teemupekka Virtanen

Professor Arto Karila

Instructor: Olavi Lallukka

**Author:** Kari Klemetti**Name of the Thesis:** Authentication in Extranets**Date:** 2001-07-25**Number of pages:** 87**Department:** Department of Computer Science**Professorship:** Tik-110 Computer Networks**Supervisor:** Professor Teemupekka Virtanen

Professor Arto Karila

**Instructor:** Olavi Lallukka

The need to exchange information between organisations is increasing. Virtual Private Network technology is used for creating extranets between organisations. However, old authentication mechanisms are cumbersome and difficult to use between different organisations.

New standards based on digital certificates have been developed to solve the emerging problems. Digital certificates, which are based on public key cryptography, ease the key management problems. Certificate Authorities and directory servers enable key distribution across organisational boundaries.

Trust becomes an important issue when talking about partnerships between organisations. The trust model of the implementation can be tailored to match the contract-based trust relationships of the business world.

A reference system demonstrates an implementation that answers to the new challenges. It is built using existing commercial products, which comply with the IPsec, Internet Key Exchange, X.509 digital certificate and LDAP directory standards.

**Keywords:** authentication, extranet, VPN

<b>Tekijä:</b>	Kari Klemetti	
<b>Työn nimi:</b>	Todentaminen kumppanuusverkoissa	
<b>Päivämäärä:</b>	25.7.2001	<b>Sivumäärä:</b> 87
<b>Osasto:</b>	Tietotekniikka	
<b>Professori:</b>	Tik-110 Tietokoneverkot	
<b>Työn valvoja:</b>	Professori Teemupekka Virtanen Professori Arto Karila	
<b>Työn ohjaaja:</b>	Olavi Lallukka	
<p>Organisaatioiden tarve vaihtaa informaatiota keskenään on lisääntymässä. Virtual Private Network –teknologialla luodaan kumppanuusverkkoja. Vanhat todennusmenetelmät ovat kuitenkin kömpelöitä ja vaikeakäyttöisiä useiden organisaatioiden kesken.</p> <p>Uusia, digitaalisiin varmenteisiin perustuvia standardeja on kehitetty ratkaisemaan esiin nousevia ongelmia. Julkisen avaimen kryptografiaan perustuvat digitaaliset varmenteet auttavat avaintenhallintaongelmissa. Varmenne- ja hakemistopalvelut mahdollistavat organisaatorajat ylittävän avainten jakelun.</p> <p>Luottamuksesta tulee tärkeä kysymys organisaatioiden välisissä kumppanuussuhteissa. Toteutuksen luottamusmalli voidaan räätälöidä vastaamaan sopimuksiin perustuvaa liike-elämän luottamusmallia.</p> <p>Esimerkkijärjestelmä esittelee toteutuksen, joka vastaa esille nousseisiin haasteisiin. Se on rakennettu käyttäen standardeihin (IPsec, Internet Key Exchange, X.509 digitaalinen varmenne ja LDAP hakemistopalvelu) perustuvia kaupallisia tuotteita.</p>		
<b>Avainsanat:</b>	kumppanuusverkko, todentaminen, VPN	

# Preface

This thesis has been written at Tecnomen Corp. as a research project. The goal of the research project was to come up with an elegant solution for maintenance connections. Tecnomen's main office and support resources are in Espoo, Finland. Installed systems can be found in fifty countries all around the world.

The work for this thesis started already in the beginning of the year 2000. The first year was utilised to gather background information and experience of firewalls and Virtual Private Networks. The actual research for this thesis was completed during the first six months of 2001.

I would like to thank Professor Arto Karila for invaluable comments and input on the content of this thesis and Olavi Lallukka for inspiration in the field of computer and network security. I would like to thank Professor Teemupekka Virtanen for helping me to finish this thesis. I also thank Kristiina Volmari-Mäkinen, Ronja Addams-Moring and Elizabeth Heap-Talvela for helping with the grammar of this thesis.

Additionally I especially thank Reetta Klemetti for supporting me in many ways when writing this thesis and believing that it would eventually be finished.

Lopuksi haluan kiittää ennen kaikkea vanhempiani, Esteri ja Oiva Klemettiä, kaikesta siitä vuosikymmeniä kestäneestä tuesta, mikä on tehnyt tämän diplomityön kirjoittamisen ylipäänsä mahdolliseksi.

Otaniemi, 25th July 2001

Kari Klemetti

# Table of Contents

<b>Abstract</b> .....	<b>ii</b>
<b>Tiivistelmä</b> .....	<b>iii</b>
<b>Preface</b> .....	<b>iv</b>
<b>Table of Contents</b> .....	<b>v</b>
<b>Definitions of Terms</b> .....	<b>ix</b>
<b>1. Introduction</b> .....	<b>1</b>
1.1 Background .....	1
1.2 Motivation.....	3
1.3 Virtual Private Network.....	3
1.4 Distributed and Mobile Work Environments .....	4
1.5 Partner Networks .....	5
<b>2. Problem Statement</b> .....	<b>6</b>
2.1 Objective .....	6
2.2 Scope.....	6
<b>3. Criteria</b> .....	<b>7</b>
3.1 Algorithm.....	7
3.2 Protocol.....	8
3.3 Implementation.....	10
<b>4. Generic Model</b> .....	<b>12</b>
4.1 Authentication Model .....	12
4.1.1 Something Known.....	12
4.1.2 Something Possessed .....	14
4.1.3 Something Embodied .....	17

4.2	Trust Model .....	18
4.2.1	Certificate .....	18
4.2.2	Certification Authority .....	23
4.2.3	Public Key Infrastructure and Trusted Third Parties .....	23
4.2.4	Trust Hierarchy.....	24
4.3	Business World .....	27
4.3.1	Certification Practice Statement and Certificate Policy .....	27
<b>5.</b>	<b>Technologies.....</b>	<b>29</b>
5.1	Authentication Mechanisms .....	29
5.1.1	Passwords .....	29
5.1.2	Transport Layer Security.....	30
5.1.3	IPsec .....	30
5.2	Virtual Private Network.....	34
5.3	Public Key Infrastructure.....	35
5.3.1	X.509 Certificates .....	35
5.3.2	Certificate Authority.....	37
5.3.3	Certificate Validation .....	38
5.4	LDAP Directory.....	39
5.5	Secure DNS .....	39
<b>6.</b>	<b>Products.....</b>	<b>41</b>
6.1	Product Categories .....	41
6.1.1	Virtual Private Network .....	41
6.1.2	Certificate Authority.....	44
6.1.3	LDAP Directory .....	47
6.2	Virtual Private Network Evaluation .....	48
6.2.1	CheckPoint FW-1/VPN-1.....	48
6.2.2	PGP Gauntlet Firewall/VPN.....	49
6.2.3	Symantec Enterprise Firewall/VPN .....	49
6.2.4	FreeS/WAN .....	49
6.2.5	Virtual Private Network Feature Matrix.....	50
6.3	Certificate Authority Evaluation.....	50

6.3.1	CheckPoint Certificate Manager .....	51
6.3.2	RSA Keon Sentry CA.....	51
6.3.3	iPlanet Certificate Management System .....	51
6.3.4	Certificate Authority Feature Matrix.....	51
6.4	LDAP Directory Evaluation .....	52
6.4.1	RSA Keon Sentry CA.....	52
6.4.2	iPlanet Directory Server .....	52
6.4.3	IBM SecureWay Directory.....	53
6.4.4	LDAP Directory Feature Matrix .....	53
<b>7.</b>	<b>Reference System.....</b>	<b>54</b>
7.1	Architecture .....	54
7.2	VPN Gateway.....	55
7.3	Certificate Authority.....	56
7.3.1	Administration Server .....	57
7.3.2	Enrollment Server.....	57
7.3.3	SCEP Server .....	57
7.3.4	CRL Server .....	58
7.4	LDAP Directory.....	58
7.5	VPN Authentication.....	59
7.5.1	VPN Gateways .....	59
7.5.2	VPN Clients .....	59
7.6	Trust Hierarchy.....	60
7.6.1	VPN Gateways .....	60
7.6.2	VPN Clients .....	60
<b>8.</b>	<b>Analysis.....</b>	<b>61</b>
8.1	Criteria .....	61
8.2	Authentication Model .....	64
8.3	Trust Model .....	65
8.4	Business World .....	66
<b>9.</b>	<b>Conclusions .....</b>	<b>67</b>

9.1 Tecnomen Maintenance Connections .....	67
9.2 Future Work .....	68
9.2.1 Advanced Encryption Standard .....	68
9.2.2 Smart Cards .....	68
9.2.3 FreeS/WAN .....	68
9.2.4 Biometrics.....	69
<b>References.....</b>	<b>70</b>
<b>Appendix A Reference System Specifications .....</b>	<b>75</b>
VPN Gateway.....	75
Certificate Authority .....	76

# Definitions of Terms

*Authentication* means in this thesis verifying that the claimed identity is valid. See also identification.

*Authentication Header (AH)* is a protocol that authenticates IP packets. See also IPsec and Security Association. [19]

*Authorisation* means in this thesis verifying that an identity has the right to perform an action. See also identification and authentication.

A *certificate* is a statement about the subject of the certificate. The certificate is signed by an issuer. See also Certification Authority.

A *Certificate Revocation List (CRL)* is a list of revoked certificates that are no longer valid.

A *Certification Authority (CA)* is an entity that issues certificates.

A *digital signature* is a hash (see hash function) that is encrypted with a private key (see private key) and can be verified with the corresponding public key (see public key).

*Encapsulating Security Payload (ESP)* is a protocol that encrypts and authenticates the payload of IP packets (see also IPsec and Security Association). [20]

An *extranet* is an extension of an organisation's intranet (see intranet) that allows partner organisations limited access to private data over the Internet. [9]

A *hash function* generates fixed length output from variable length input. Hash functions are one-way (original input can not be deduced from the output) and collision free (an input that generates the desired output is hard to find).

*Identification* means discovering the identity.

*Internet Key Exchange* (IKE) is a protocol that defines authentication and key exchange based on ISAKMP and Oakley. See Internet Security Association and Key Management Protocol and Oakley. [12]

*Internet Security Association and Key Management Protocol* (ISAKMP) is a framework for establishing Security Associations and cryptographic keys in an Internet environment. See Security Association. [28]

An *intranet* is a network that provides services similar to those provided by the Internet but which is private inside an organisation. [9]

*IPsec* is a security architecture containing a suite of protocols and algorithms that provide security services at the IP layer. [21]

A *Keyed-Hash Message Authentication Code* (HMAC) is a message authentication code (see Message Authentication Code) that uses a keyed hash function (see hash function). The keyed hash function incorporates a secret key in calculating hash values.

*Message Authentication Code* (MAC) is a mechanism for authenticating messages using cryptography.

*Oakley* is a protocol for two authenticated parties to agree on secure and secret keying material. [32]

*Opportunistic encryption* is used in a Virtual Private Network connection, when the endpoints cannot verify the identity of each other. See Virtual Private Network. [10]

*Perfect Forward Secrecy* (PFS) means that the key used to protect the transmission of data is not used to derive any additional keys. [12]

A *private key* is the secret part of the key pair that combined with the public key (see public key) can be used to provide the security services of public key cryptography.

A *public key* is the public part of the key pair that combined with the private key (see private key) can be used to provide the security services of public key cryptography.

*Public Key Infrastructure* (PKI) is an infrastructure that supports the applications of public key cryptography.

*Secure DNS* is an extension to Domain Name Service (DNS) that provides storage for public keys and digital signatures. [6]

A *Security Association* (SA) is a simplex connection that affords security services to the traffic carried by it. [21]

A *Trusted Third Party* (TTP) is an entity that is trusted. Certification Authorities are specialised Trusted Third Parties (see Certification Authority).

A *Virtual Private Network* (VPN) is a mechanism to connect distributed local area networks into one big logical network. The connection is secure even across public, insecure networks such as the Internet.

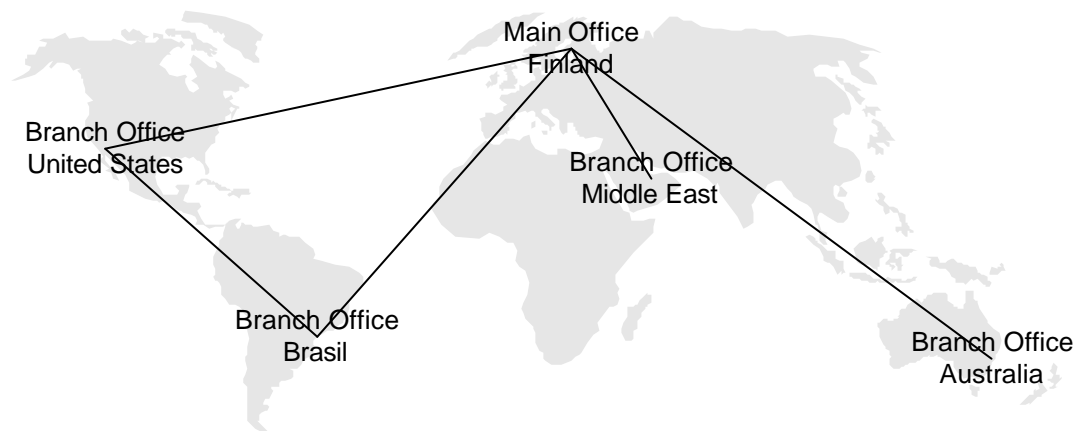
A *Virtual Private Network gateway* is a relay on the edge of the Virtual Private Network, which encrypts and authenticates outbound messages and relays them to a peer Virtual Private Network gateway.

# 1. Introduction

This chapter gives a brief introduction to the background of the problem field and to the motivation of this thesis.

## 1.1 Background

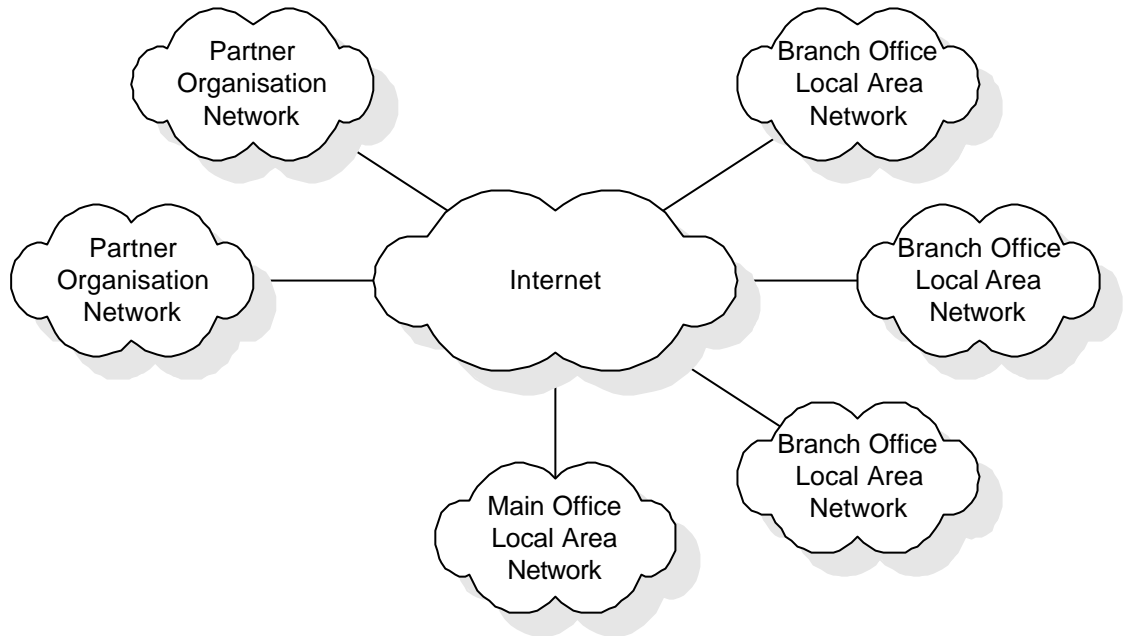
Organisations depend on information more and more nowadays. For the information to be easily accessed and exchanged, it is stored in computer systems. New business models and out-sourcing of services require much more flexible exchange of information than before. The offices of an organisation are often geographically distributed all over the world (see Figure 1 below), yet the information should be easily accessed and exchanged.



*Figure 1. Geographically distributed offices of an organisation.*

Organisations have partner organisations that they want to give access to some part of their information system in exchange of business benefits. In global partnership networks, organisations have different partners each in different field of operation. Thus the organisations must have an easy and flexible way of controlling what information is accessible and by whom.

Most organisations have already connected themselves to the Internet. Business-to-consumer operations are increasingly performed over the Internet. Recent development has been that also the business-to-business operations are transferred to use the Internet as a transport mechanism (see Figure 2 below).



**Figure 2.** Organisation's network and partner networks distributed over the Internet.

The Internet is a public, insecure network. Anyone can connect to the Internet. Basically all information sent to the Internet is public. The information can be read by anyone who happens to be on the information flow path. Internet operators and national security agencies have access to all information in the part of the Internet that they govern.

The information exchanged between partner organisations is often confidential and of monetary importance. The information must not fall into competitors' hands. The exchange of information must be secure. It must not be possible for any unauthorised party to eavesdrop the information or to gain access to the information.

The exchange of information can be performed in a secure way. The information can be encrypted and authenticated whenever leaving the organisation's information system to the Internet and decrypted and verified whenever entering into the partner organisation's information system. This way the information is transferred in encrypted form over public, insecure networks.

## **1.2 Motivation**

The specific application in this thesis is to create secure maintenance connections between a vendor (Tecnomen) and the customers (teleoperators). Tecnomen manufactures value added service platforms. Teleoperators purchase the platforms to give value added services to their customers.

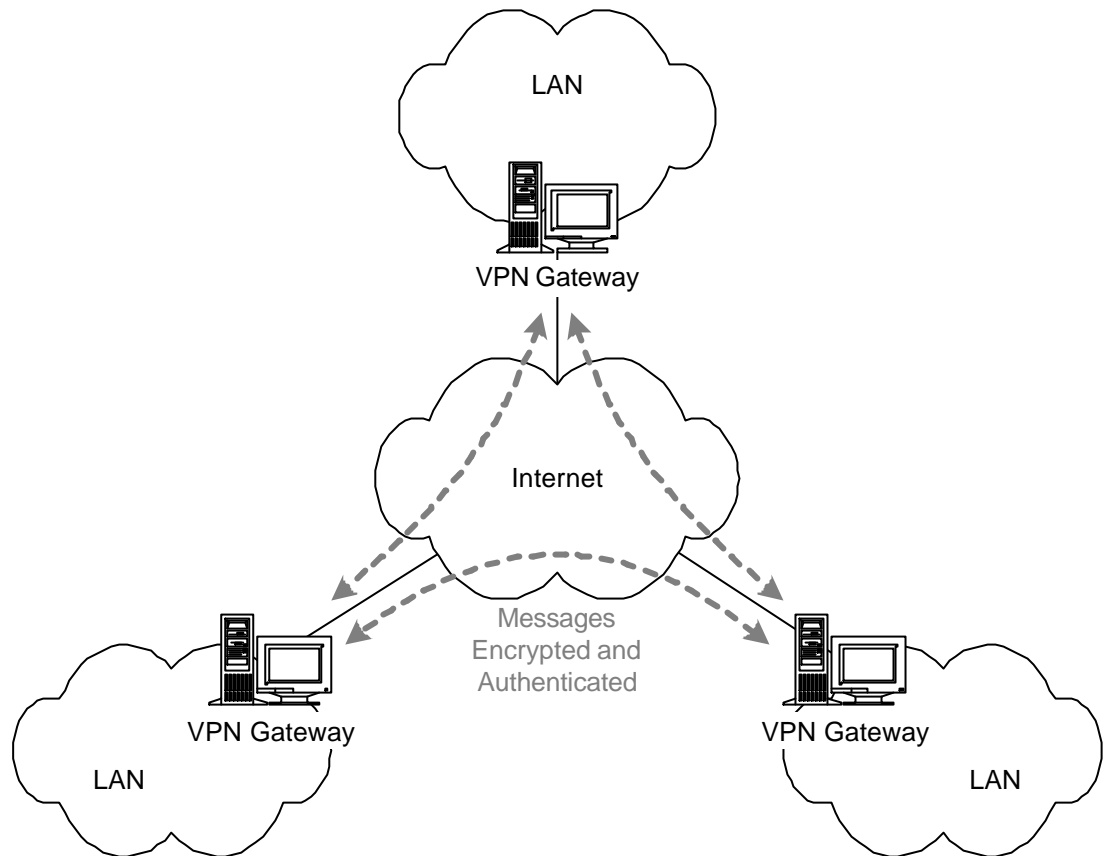
The teleoperators are reluctant to give access to their information system across public, insecure networks such as the Internet. Teleoperators must be assured that the mechanisms and procedures used are robust and cryptographically strong. The authentication trust model must be particularly robust.

Despite the specific application area, much care has been taken to ensure that the implementation and analysis in this thesis is generic. The implementation and analysis should be valid wherever partner organisations need to exchange information.

## **1.3 Virtual Private Network**

Virtual Private Network technology has been used in many organisations to connect geographically distributed offices transparently in a secure way. Usually the office's local area networks are isolated from the Internet by a firewall.

Inside the firewall there is a Virtual Private Network gateway that relays the traffic going to another office to a peer Virtual Private Network gateway that is located in the other office. The messages in transit between Virtual Private Network gateways are encrypted and authenticated. See Figure 3 on page 4 for illustration.



**Figure 3.** *Virtual Private Network.*

## 1.4 Distributed and Mobile Work Environments

Work environments in organisations are becoming more distributed and mobile. This means that an increasing number of users require access to the organisation's information system from home or while on the road. This requirement imposes several security threats to the security of the organisation's information system.

Access to the organisation's information system must be controlled. Access is allowed only to authorised distributed offices and mobile workers. The distributed offices and mobile workers must be authenticated using strong cryptography.

The same mechanism that is used to connect distributed offices and mobile workers to organisation's information system can be used to allow access to partner organisations. Partner organisation is treated like one distributed office or mobile worker.

## 1.5 Partner Networks

There are some special issues with partner networks. The access to the organisation's information system must be limited. Partner organisations do not generally require full access to the entire information system. It must be possible to limit the extent of the access.

Virtual Private Network can be used to restrict access to specific subnetworks. Additionally all the normal information system access control mechanisms found in operating systems and applications can be used.

## **2. Problem Statement**

The problem is to authenticate users and services from other partner networks in a structured manner. Structured manner means that an organisation may define an individual access policy for each partner organisation.

Different partner organisations have different business needs. Different partners require access to different parts of the information system or require different access rights to the information system. Still, for simplicity, there should be only one authentication mechanism for all partner organisations.

### **2.1 Objective**

The main objective of this thesis is to build an authentication mechanism that supports a multi-organisational extranet. The authentication mechanism is built by integrating existing third-party products. In addition to the authentication mechanism, supporting functions must also be implemented but they are not the main concern.

### **2.2 Scope**

The scope of this thesis is limited to building the authentication mechanism for a data network that uses the IP protocol family. The mechanism is intended particularly for the Internet.

This thesis does not address firewalls although many third party commercial products tightly couple firewalls and Virtual Private Network gateways. In this thesis firewalls are used for access control, not for authentication.

## 3. Criteria

This chapter describes the criteria that the authentication mechanism must fulfil to be a useful and successful system.

### 3.1 Algorithm

The authentication mechanism must be strong because organisations have confidential information in their intranets, which they do not want to fall into their competitors' hands.

**Criterion 1** The algorithms must use strong cryptography.

The specifications of the algorithm must be public. The security of the algorithm must not rely on the secrecy of the specifications i.e. security through obscurity. Secret specifications have the tendency that they will not stay secret for long.

If the specifications are secret then it is possible that the specifications contain backdoors or other malicious design that deteriorate security. The specifications of the algorithm must have been publicly available for several years. The academic community and the public have had enough time to verify the security of the design.

The algorithms must have been widely used for several years. Continuous wide use implies that the people, who design the applications, and the people, who use the applications, believe that the algorithms are secure.

**Criterion 2** The algorithms must use strong keys.

The key length must be so long that it is unfeasible to make a brute force attack against the algorithm. The brute force attack can be either a known plaintext or a chosen plaintext attack.

The required computational resources or the required memory resources must be several orders of magnitudes higher than the estimated resources that any organisation could have.

The algorithm must also be secure for some time into the future. A brute force attack must be unfeasible also in the years to come. Depending on the sensitivity of the data the time frame can be a year or two or even ten years.

Moore's law says that the computational and memory resources double every 18 months. According to that law computational and memory resources grow hundred-fold in ten years.

## 3.2 Protocol

The authentication mechanism must provide the authentication service, it must not have design flaws and it must be easy to use.

**Criterion 3** The protocol must implement Virtual Private Network at IP level.

The easiest way to introduce security to any system is when the users do not have to do any additional actions to enhance the security. All old applications work the same way as they have worked before.

The only way to do this is to implement the Virtual Private Network at IP level. After the Virtual Private Network is set up, it will be completely transparent to the end user.

**Criterion 4** No plaintext authentication tokens (passwords etc.) must pass across insecure networks.

The protocol must not rely on the security of the network. The protocol must be secure even if the attacker can listen to the network traffic.

If an unauthorised party can acquire the authentication tokens for example by eavesdropping the communications channel, it could use the authentication tokens to impersonate as legitimate user and gain unauthorised access.

**Criterion 5** The protocol must provide confidentiality, integrity and protection against replay attacks.

Unauthorised parties must not be able to eavesdrop the information that is transmitted to the network. The information must be encrypted to ensure confidentiality.

The information sent to the network must be tamper-proof. The integrity of the information must be maintained. This is accomplished by authenticating the data.

The exchange of information must be secure against replay attacks. An eavesdropper might record a stream of information and might resend it at a later time. This attack must be detected and the unauthorised stream of information must be discarded.

**Criterion 6** The protocol must provide authenticated keying material that is kept confidential.

The protocol must provide keying material. The keying material is used to initialise the encryption and authentication algorithms. The keying material must be kept confidential against eavesdroppers.

The keying material must be authenticated so that the communication parties can be sure of the identity of each other. Not even a man-in-the-middle attacker can divert the key exchange to acquire the keying material.

### 3.3 Implementation

The implementation of the authentication mechanism must be solid, robust, easy to administer and cost efficient.

**Criterion 7** The complexity of key management must be at most linear as the number of parties increase.

In small systems the connections between end points can be configured manually. The number of configured connections grows exponentially as the number of end points increase.

Large systems require easy key management. The connections must be configured automatically. When setting up a large system the complexity of the key management must be based on the number of end points, not on the number of separate connections.

**Criterion 8** The protocol must provide Perfect Forward Secrecy.

Perfect Forward Secrecy means that the compromise of a single key restricts the security breach only to data protected by that key.

To facilitate Perfect Forward Secrecy the key used to protect transmission of data is not used to derive any additional keys.

**Criterion 9** The administrator of a network must be able to decide which partner networks are permitted access.

Organisation offering its intranet to the partner organisations must have the means to define what partners have access to what information.

The authentication mechanism can be quite complex because the trust relationships of each partner are different.

**Criterion 10** The system must be built using already existing products.

It is very important that security products do not contain any bugs that would result in a security breach. Companies that produce security products have comprehensive experience about secure coding and testing guidelines. It would be infeasible for the inexperienced to try to make such a critical product from scratch.

Existing products also have an established customer base, which has tested the product in different real world environments. Special cases in such real world environments are hard to test or even foresee.

In addition the cost of making a security product by oneself is much higher than buying one from the store. There are organisations, however, who require access to full source code and for which buying existing security products is not an option.

## 4. Generic Model

This chapter describes the theoretical background of the problem statement. The theory behind different aspects of the problem field and possible solutions is important knowledge when designing a solution.

### 4.1 Authentication Model

Authentication can be based on different types of authentication tokens. Authentication tokens are normally categorised in three categories: something known, something possessed and something embodied [1].

The following sections explain each category in detail. The sections describe the theory, examples, feasibility and future prospects of the authentication token category.

#### 4.1.1 Something Known

The subject of the authentication knows some piece of information that can be used to reliably verify that the identity of the subject is what it claims to be. It is of utmost importance that no one else does know the same piece of information nor can guess it. The authentication token is a secret and should be protected against exposure.

##### **Password**

The most common application of this authentication token category is a password. A username is used in conjunction with a password to perform both identification and authentication. Username/password authentication is widely used because it is easy to implement and easy to use.

Commonly used passwords are the exact same string as the username or the name of the user or user's spouse, cat or dog. Also an empty password is very common. This kind of passwords conflicts directly with the requirement that nobody should be able to guess it. There have been several attempts to improve the security of username/password authentication by enforcing good passwords. The password is typically required to be at least six characters in length and to include numbers and special characters. The password is also checked against a dictionary of names, words and word combinations.

It is also good for the user to have different password in every system. The exposure of one password is restricted to one system. The requirement of distinct passwords leads to the situation where user has many passwords, each hard to guess and thus hard to remember, and the user have to write them down to notes or notebook. Writing passwords down is again a bad idea. If the note or notebook is lost or stolen, then there is a possibility of a security breach.

## **PIN**

Different variants of passwords are also used. Personal identity number or PIN is used for weak authentication to protect physical devices e.g. credit cards or mobile phones.

## **Passphrase**

The term passphrase is used to describe an alternate form of password. Passphrase is a phrase that consists of several words, spaces, capital letters and special characters. Passphrases are considered as good passwords because they are long and thus hard to guess and still easy for the user to remember.

## **Feasibility**

The reliability of the 'something known' authentication scheme depends on the confidentiality of authentication tokens and on the difficulty of guessing them. Depending on the application different kinds of passwords can be used. However, in systems where high level of security must be achieved, passwords do not provide strong enough authentication.

In addition to trying to guess a password, a brute force attack can be used. The brute force attack tries all possible combinations. Password's resistance against the brute force attack depends on the number of possible combinations. The number of possible combinations then again depends on the length of the password. Longer passwords are harder to crack.

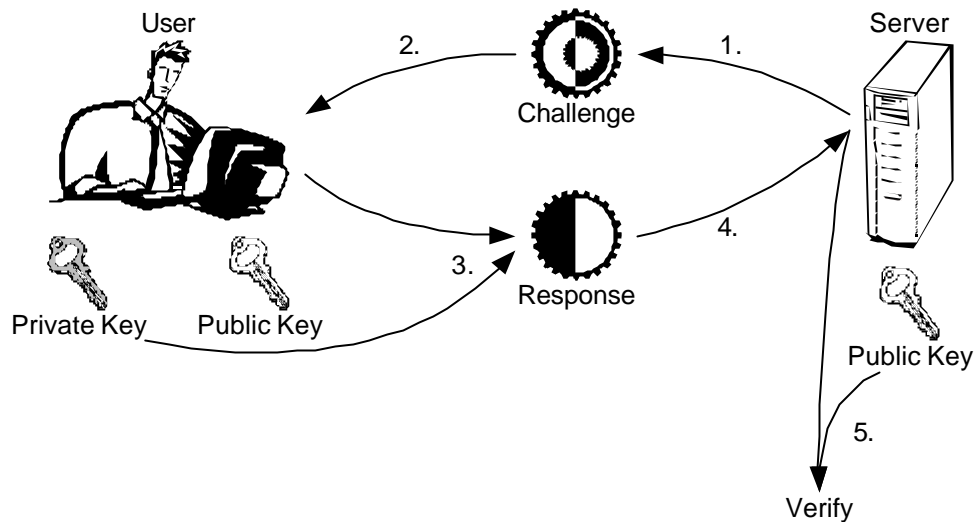
### **4.1.2 Something Possessed**

The subject of the authentication possesses an authentication token that can be used to reliably verify that the identity of the subject is what it claims to be. It is of utmost importance that no one else can get access to the authentication token and nor can steal it. The authentication token is a secret and should be protected against theft.

The ownership of the authentication token can be verified by using a challenge-response exchange.

1. The authenticating party creates a challenge.
2. The challenge is sent to the subject of authentication.
3. The subject of authentication creates a response from the challenge and the authentication token.
4. The response is sent back to the authenticating party.
5. The authenticating party verifies that the response was created from the challenge and the authentication token.

The authentication tokens in challenge-response exchange can be a shared secret (symmetric cryptography used for example in GSM phone authentication) or private and public keys of the subject of authentication (asymmetric cryptography used for example with certificates). A private and public key challenge-response exchange is illustrated in Figure 4 on page 15.



**Figure 4.** A challenge-response exchange.

### Private Key

Public Key Infrastructure uses key pairs. The keys in the key pair are large random numbers. One of the keys is a private key that must be kept secret and the other is a public key that can be published in a public place.

The party that wants to authenticate another party can issue a challenge-response exchange. The challenge and the response are large random numbers. The subject of the authentication creates the response from the challenge with the private key. The authenticating party can verify the response with the public key and the original challenge.

Based on the complex mathematical relationship between private key and public key, the correct response can be constructed only with the private key. The private key cannot be constructed from the public key.

Public Key Infrastructure can be used to verify the possession of the private key. The reliability of the authentication depends on how well the private keys are protected.

## **Security Device**

Security devices are physical devices that contain a secret piece of information. The secret piece of information can be either a shared secret (symmetric cryptosystem) or private key (asymmetric cryptosystem).

The security device is used in the challenge-response exchange in the same way as a private key. The challenge is input to the security device, which calculates the response from the challenge and the secret piece of information. The security device gives the response as output.

Challenge-response exchanges can be used to verify the possession of a security device. The reliability of the authentication depends on how well the security device is protected. Security devices have different kinds of protections against tampering so that the secret piece of information could not be extracted from the security device even if the security device is disassembled.

## **Smart Card**

Smart cards are a special form of security devices. The security device is a chip on a normal credit card. Smart cards are becoming increasingly common and are replacing traditional security devices because smart cards are based on widely adopted standards.

## **Feasibility**

Private keys, security devices and smart cards have additional level of protection against if they are lost or stolen. Passwords, passphrases or PINs are used depending on the security requirements of the particular application.

Public Key Infrastructure and smart cards facilitate the wide adoption of strong authentication. Shared secrets is not a feasible authentication method when systems are large. The number of shared secrets grow exponentially based on the number of subjects but the number of authentication tokens in Public Key Infrastructure or smart cards grow linearly.

### **4.1.3 Something Embodied**

Authentication of a human being can also be based on the physiological characteristics of the human being. The subject of the authentication is checked to have the specified physiological attribute.

#### **Fingerprint**

Fingerprints have been used for a long time to solve crimes. All human beings have distinct fingerprints. Authentication can be based on accurately reading the fingerprints of a human being and comparing the results to reference fingerprints.

#### **Retina Scan**

All human beings have distinct eye retinas. Authentication can be based on accurately reading the retina of a human being and comparing the results to reference retina.

#### **Voice Identification**

All human beings have a distinct voice. Authentication can be based on analysing the characteristics of the voice of a human being and comparing the results to reference characteristics of the voice.

#### **Signature Style**

All human beings have a distinct way of writing their signature. The characteristics of the rhythm and pressure changes of the signing can be analysed. Authentication can be based on comparing the results to characteristics of the reference signature style.

#### **Feasibility**

The reliability of authentication based on human physiological characteristics is very much depending on the accuracy of reading the physiological characteristics. Some desktop appliances doing authentication based on user's fingerprints are commercially available. As a rule of thumb the following can be used: the reliability of the authentication goes very much hand-to-hand with the cost of the system.

It has also been argued that ‘something embodied’ can be stolen. It is possible to record the voice of subject and then play it to the authentication system. In theory somebody could even cut the subject’s hand or take the subject’s eye and use it to the authentication system. These kinds of issues must be taken into consideration when designing and implementing authentication systems that are based on physiological characteristics.

It would be nice to have reliable authentication based on for example voice identification. Logging on to a computer could be done just by saying ‘Hello!’ to the computer. Unfortunately nowadays this is only science fiction.

Perhaps the most promising mechanism is the signature style recognition. The cost and accuracy of pressure sensitive pads is reasonable. The technology is not yet mature enough but perhaps in few years we log on to a computer by giving a signature.

## **4.2 Trust Model**

Trust is what authentication is all about. The password that a legitimate user enters to a computer system is trusted not to be compromised, but is only known by the legitimate user. The private key, the security device or the smart card of a legitimate user is trusted not to be stolen. Additionally even if it is stolen, it is protected by the password, passphrase or PIN.

The trust that is addressed in this section deals with the trust relationships in Public Key Infrastructure. The trust relationships are expressed with certificates in Public Key Infrastructure.

### **4.2.1 Certificate**

A certificate has a subject, for whom the certificate is created for and an issuer, who creates the certificate. In Public Key Infrastructure a certificate contains the following mandatory parts:

1. Information about the subject

2. Subject's public key
3. Issuer's signature
4. Issuer's public key

The information about the subject can be identification (identity certificates), a right to perform an action (authorisation certificate) or designation to a group (role certificate) or any statement that the issuer wants to sign (generic form of a certificate). Identity certificates are the most common type of certificates used today.

The certificates usually have validity period, which states when the certificate expires. The issuer of certificates also issues periodically certificate revocation list, which contains all revoked certificates. Before accepting a certificate it should be verified from the certificate revocation list that it is not on the black list.

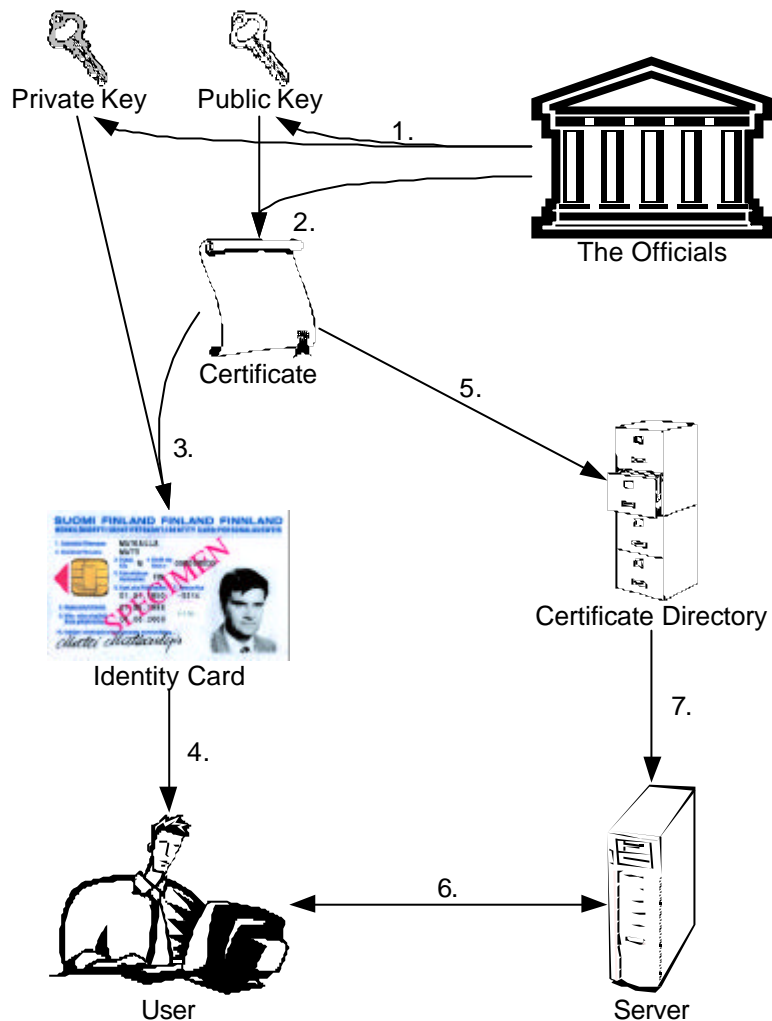
The semantics of an identity certificate is that the issuer states that the public key belongs to the identity. The officials ultimately define the identity of a person by issuing an identity card.

### **Official Identity Certificate**

The officials can issue an identity certificate as follows (see Figure 5 on page 20):

1. The officials create a public key and a private key.
2. The officials issue a certificate binding the public key to an identity.
3. The officials issue an identity card containing the keys, the certificate and identification information.
4. The identity card is delivered to the user. No copies of the private key is stored elsewhere.
5. The officials publish the certificate in a public directory.
6. Authenticating party can authenticate the user with challenge-response exchange.

7. Authenticating party can verify the response by downloading the certificate from the public directory.



*Figure 5. The officials issue an identity certificate.*

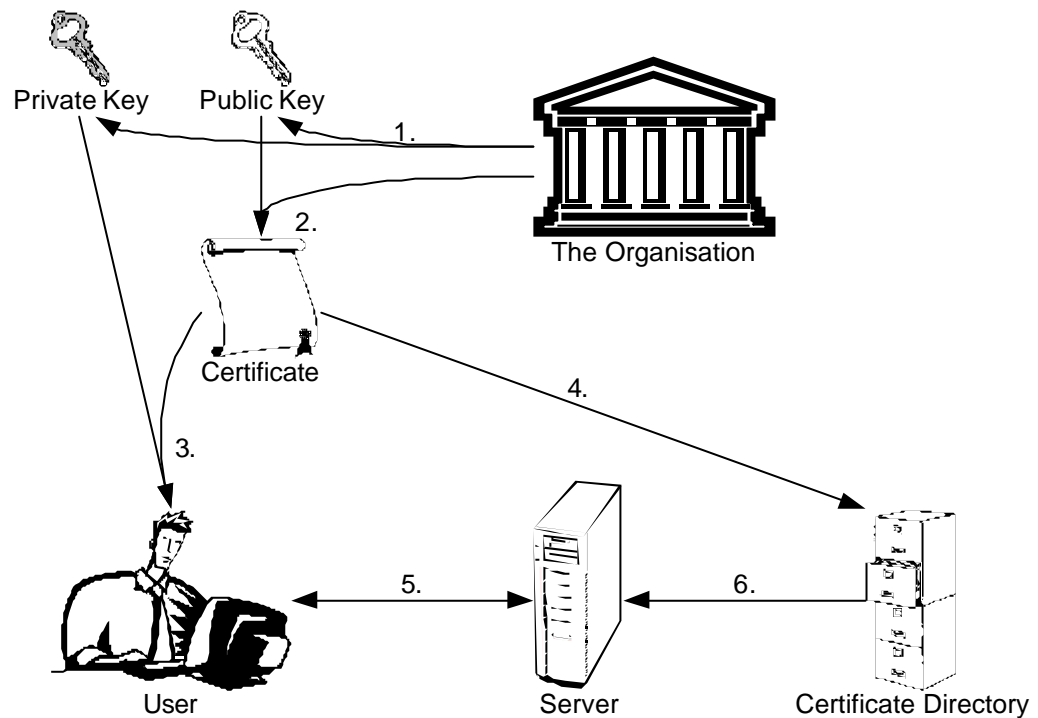
### Other Identity Certificates

The identity certificate issued by the officials can be used for strong authentication in any application. There are, however, political and business reasons for other organisations to issue their own identity certificates.

The issuer of an identity certificate uses different kinds of controls to verify the identity of the subject. Perhaps the most common control is that the person gets the identity certificate against an official identity card.

An organisation can issue an identity certificate as follows (see Figure 6 on page 21):

1. The organisation creates a public key and a private key.
2. The organisation issues a certificate binding the public key to an identity.
3. The identity certificate is delivered to the user. The identity of the user is verified by using official identity card. No copies of the private key is stored elsewhere.
4. The organisation publishes the certificate in a public directory.
5. The server can authenticate the user with challenge-response exchange.
6. The server can verify the response by downloading the certificate from the public directory.



*Figure 6. An organisation issue an identity certificate.*

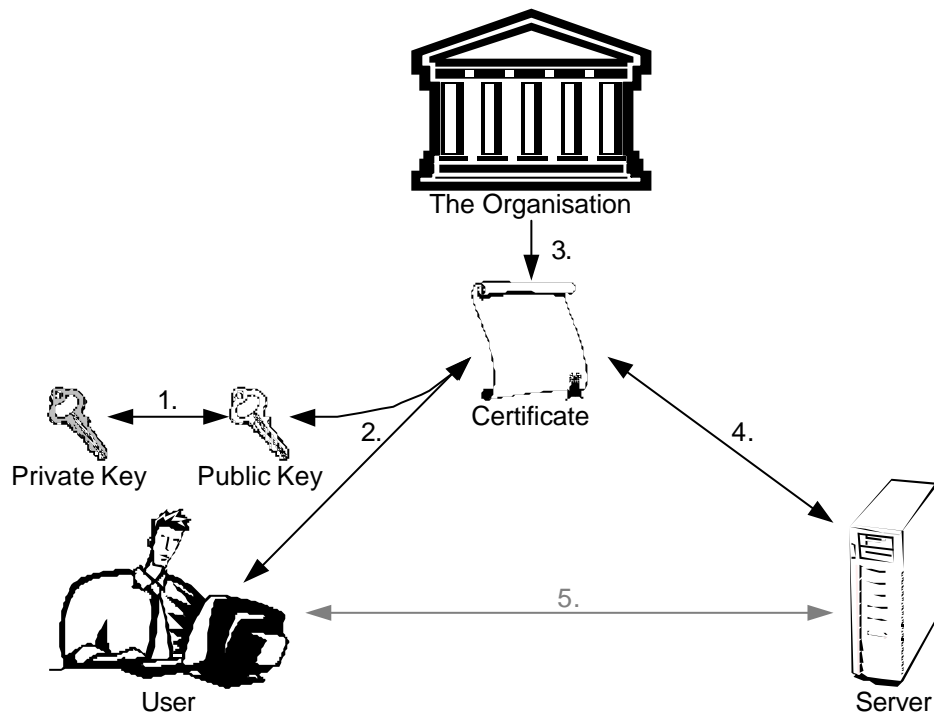
### Chain of Trust

The chain of trust can be modelled with private keys, public keys, certificates and challenge-response exchanges. The following prerequisites must be in place before the chain of trust is complete:

1. The person possesses a private key, a public key and an identity certificate issued by the organisation.
2. The server possesses the public key of the organisation.

The chain of trust goes like this (see Figure 7 below):

1. The private key is cryptographically bound to the public key.
2. The identity certificate binds the identity of the person to the public key.
3. The identity certificate is signed by the organisation.
4. The server can verify the signature on the person's identity certificate with the organisation's public key.
5. The server can verify the possession of the person's private key using challenge-response exchange.



**Figure 7.** Chain of trust.

## **4.2.2 Certification Authority**

The entity that issues certificates is called Certification Authority. It is important that the subjects of certificates issued by the Certification Authority must trust the Certification Authority.

The responsibilities of a Certification Authority include:

1. Receive certificate requests.
2. Verify the identity of the subject of a certificate.
3. Issue certificate.
4. Revoke certificates.
5. Publish certificate directory.
6. Publish certificate revocation list.

## **4.2.3 Public Key Infrastructure and Trusted Third Parties**

Public Key Infrastructures can be categorised as three categories: open, open-but-bounded and closed.

### **Open Public Key Infrastructure**

Open Public Key Infrastructure is open to everyone. Anyone can join and start using the existing infrastructure.

One example of open Public Key Infrastructure is the X.509 certificate directory structure used in Internet browsers' SSL/TSL. Certification Authorities include Microsoft, Saunalahti, SecureNet, TC TrustCenter, ValiCert and VeriSign.

### **Open-but-bounded Public Key Infrastructure**

Open-but-bounded Public Key Infrastructure is public but it is restricted to specific group of subjects. Certification Authorities are entities that have already established trust to the public.

The officials issue electronic identity cards. Teleoperators issue certificates that can be used for digital signatures in mobile phone subscriber identity modules. Credit card companies or banks issue certificates for electronic transactions.

### **Closed Public Key Infrastructure**

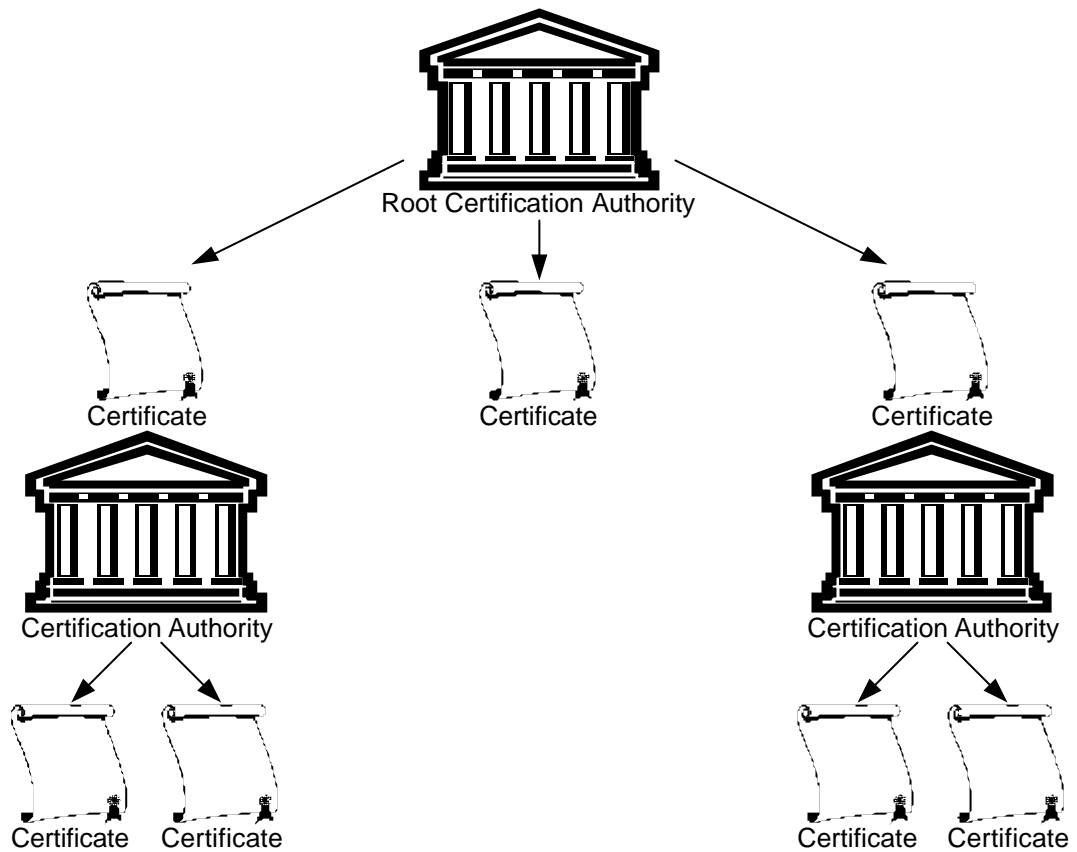
Closed Public Key Infrastructure is not public and is restricted inside an organisation or within few partner organisations. There the organisation itself is the Certification Authority and all subjects trust the organisation.

As a Certification Authority the organisation can issue identity, authorisation or role certificates to its members. The authentication and authorisation mechanisms can be based on these certificates.

It may be possible that in a closed Public Key Infrastructure the identity certificate is considered as an identity card. In this case the certificate implicitly state that the issuer trusts the subject.

#### **4.2.4 Trust Hierarchy**

In its simplest form trust hierarchy consists of a Certification Authority and certificates issued by the Certification Authority. However, it is possible to have multiple levels of Certification Authorities. In this case the root Certification Authority issues certificates to other Certification Authorities. See Figure 8 on page 25 for illustration.

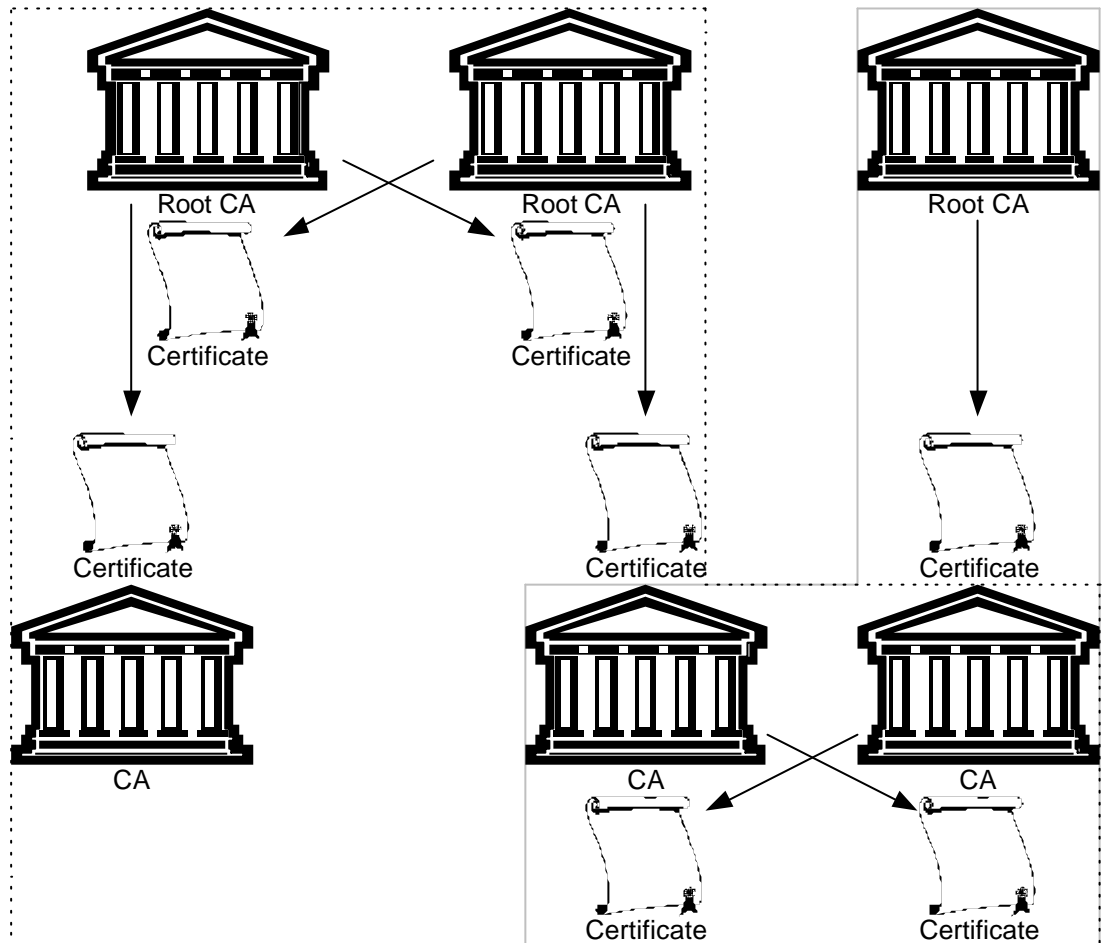


**Figure 8.** *Multilevel trust hierarchy.*

The certificates of the root Certification Authority and the certificates of other Certification Authorities can be used in the same Public Key Infrastructure. Open Public Key Infrastructures often use multilevel trust hierarchy in order to make large Public Key Infrastructures manageable.

In addition to multilevel hierarchy of Certification Authorities, a Certification Authority can issue a certificate also to other Certification Authorities. This is called cross certification. In the case of cross certification it is possible to have multiple root Certification Authorities. The cross certification is also possible at any level of the trust hierarchy. If the cross certification is made at a lower level, the preceding Certification Authorities of the cross certified Certification Authorities are in different Public Key Infrastructures.

Trust exists only inside a Public Key Infrastructure. Only the certificates issued by a trusted Certification Authority are valid. If the trusted Certification Authority has issued certificates for other Certification Authorities, the certificates issued by those Certification Authorities are also valid.



**Figure 9.** Cross certification.

There are two cross-certified root Certification Authorities in Figure 9 above. The root Certification Authorities have both issued a certificate for a sub Certification Authority each. The right one of the sub Certification Authorities has cross-certified another Certification Authority. This as a whole is one Public Key Infrastructure.

There is another Public Key Infrastructure in Figure 9 above. The rightmost root Certification Authority has issued a certificate for one sub Certification Authority. The sub Certification Authority has cross-certified another Certification Authority. This as a whole is also one Public Key Infrastructure.

It is important to note that the same Certification Authority can belong to multiple Public Key Infrastructures in this kind of lower-level cross-certified Public Key Infrastructure.

## **4.3 Business World**

Organisations trust their employees and employees trust their employer in work related matters. The employer can issue identity certificates to its employees and use them as a basis for an authentication system.

Two organisations can sign a contract and establish trust between each other. The organisations can then construct an extranet. Public Key Infrastructure can be used for authentication in the extranet. Both organisations have their own Certification Authorities that issue certificates for their employees.

The organisations can cross certify each other's Certification Authority so that the employees of the partner organisation can be authenticated in the extranet.

After the employees of the partner organisation can be authenticated, the authorisations given to the partner organisation's employees must be defined. Often the partner organisation's employees do not have the same access rights as the organisation's own employees.

The partner organisation's employees are authorised to use a specific part of the organisation's information system. The specific part is the services and information that is required in the partnership.

### **4.3.1 Certification Practice Statement and Certificate Policy**

The Certification Practice Statement and Certificate Policy specify the working practices and responsibilities of the Certification Authority.

The Certification Practice Statement defines the processes of issuing certificates and management practices.

The Certificate Policy defines the validity of the certificates, the applications for which the certificates can be used.

When talking about Tecnomen and the customers of Tecnomen i.e. the teleoperators, there are high requirements to the Certification Practice Statement or Certificate Policy. The teleoperators are not eager to open parts of their intranet to others.

# 5. Technologies

This chapter contains a survey of technologies that are used for authentication, encryption and secure network connections.

## 5.1 Authentication Mechanisms

### 5.1.1 Passwords

Passwords are probably the most common authentication mechanism in computers and networks. Passwords are usually accompanied with a username. Username is usually a shortened version of the name of the user. Password consists of alphabets, numbers and special characters.

Users choose normally passwords that are easy to remember. Words and names are usual passwords. Often easy-to-remember passwords are also easy to guess. As an authentication mechanism this is not a good idea. An unauthorised person can try to impersonate as an authorised user by guessing the password. Automated tools that try to guess passwords are publicly available.

Most current password authentication systems run a quality check for passwords to eliminate weak passwords that are easy to guess. It is possible to crack a password that cannot be guessed. All possible character combinations are checked. The complexity of the attack depends on the length of the password and the number of different characters that can be used.

Adequate protection can be achieved with passwords that are at least eight characters long and use alphabets, numbers and special characters. The best passwords are made of randomly chosen characters. Random passwords are, however, hard to remember. Instructions, how to make strong passwords, which are still easy to remember, are publicly available.

## 5.1.2 Transport Layer Security

Transport Layer Security (TLS) protocol [4] provides secure client/server connections across insecure networks such as Internet. TLS operates on top of some reliable transport protocol such as TCP/IP. TLS Record Protocol is used for encapsulating higher level protocols.

Transport Layer Security provides two security services:

1. Confidentiality – symmetric cryptography is used to encrypt the messages.
2. Integrity – the message integrity is ensured by using secure hash functions.

The keys used in the security services are generated uniquely for every connection by using TLS Handshake Protocol. TLS Handshake Protocol has the following functionality:

1. Authentication – identities can be authenticated using asymmetric public key cryptography such as RSA or DSS.
2. Negotiating shared secret – the shared secret is protected against eavesdroppers and man-in-the-middle attackers.

Transport Layer Security has somewhat limited applicability because it is applied on top of transport protocol. Introduction of TLS to an existing application require modifications to the source code. TLS is not transparent to the applications.

Many common protocols have been specified to be used over Transport Layer Security. Examples of TLS-secured protocols are HTTP, SMTP, SNMP, IMAP, POP3 and LDAP.

## 5.1.3 IPsec

IPsec is a suite of protocols, algorithms and procedures that provide security services at IP level. The goal of IPsec is to offer interoperable, high quality and cryptography-based security services for IPv4 and IPv6. [21]

The set of offered security services include:

1. Access control
2. Connectionless integrity
3. Data origin authentication
4. Protection against replay attacks
5. Confidentiality
6. Limited traffic flow confidentiality

IPsec suite provides the mentioned security services by two traffic security protocols, the IP Authentication Header (AH) and the IP Encapsulating Security Payload (ESP), and cryptographic key management procedures and protocols, the Internet Key Exchange (IKE).

### **Security Association**

Security Association (SA) is a one-way connection between two end points, and it describes a security service. Separate SAs are required for both directions. SA can use either AH or ESP. If both AH and ESP are applied in both directions, then four SAs are required for that connection.

SA is a triplet of Security Parameter Index (SPI), destination IP address and security protocol identifier (AH or ESP). Two types of SAs have been defined, transport mode and tunnel mode. Transport mode SA is used between two communicating hosts. Tunnel mode SA is applied to an IP tunnel. If either end of an SA is a gateway, the SA must be in tunnel mode.

### **IP Authentication Header**

The IP Authentication Header (AH) [19] protocol provides connectionless integrity (2.), data origin authentication (3.) and protection against replay attacks (4.). Access control (1.) mechanisms can be built based on the data origin authentication.

AH inserts an authentication header in each IP packet after the IP header. In transport mode the upper level protocol data is the payload. In tunnel mode the original IP packet is the payload. AH provides the security services to as much of the IP header as possible as well as for upper level protocol data. Only some mutable IP header fields that are changed in transit are not protected.

AH can be applied alone, in combination with ESP or nested in a tunnel mode. The security services can be established between two hosts, between a host and a gateway or between two gateways.

Keyed Message Authentication Codes (MACs) are used to authenticate the data. MACs can be based on one-way hash functions or symmetric cryptography in point-to-point communication. For multicast communication the one-way hash algorithms must be combined with asymmetric cryptography.

There are two mandatory authentication algorithms in the specification, MD5 [26] and SHA-1 [27]. Both of these are based on one-way hash functions.

### **IP Encapsulating Security Payload**

The IP Encapsulating Security Payload (ESP) [20] provides connectionless integrity (2.), data origin authentication (3.), protection against replay attacks (4.), confidentiality (5.) and limited traffic flow confidentiality (6.). Access control (1.) mechanisms can be built based on the data origin authentication.

ESP encapsulates the upper level protocol data with security parameters and authentication information. In transport mode the ESP encapsulates the upper level protocol payload. In tunnel mode ESP encapsulates the original IP packet. ESP provides the security services only for the payload. Also the security parameters are authenticated but not encrypted.

ESP can be applied alone, in combination with AH or nested in a tunnel mode. The security services can be established between two hosts, between a host and a gateway or between two gateways.

Symmetric encryption algorithms are used to encrypt the data. Encryption is optional; the encryption algorithm can be “null”.

Keyed Message Authentication Codes (MACs) are used to authenticate the data. MACs can be based on one-way hash functions or symmetric cryptography in point-to-point communication. For multicast communication the one-way hash algorithms must be combined with asymmetric cryptography. Authentication is optional; the authentication algorithm can be “null”.

There is one mandatory encryption algorithm, DES in CBC mode [25]. There are two mandatory authentication algorithms in the specification, MD5 [26] and SHA-1 [27]. Both of these are based on one-way hash functions. Also “null” encryption algorithm and “null” authentication algorithm are required by the specifications.

### **Internet Key Exchange**

Internet Security Association and Key Management Protocol (ISAKMP) [28] specifies a framework for authentication and key exchange. Oakley [32] and SKEME [23] specify series of key exchanges. Internet Key Exchange (IKE) [12] specifies a key exchange protocol, which uses part of the Oakley and SKEME key exchanges, in accordance to the ISAKMP framework.

IKE establishes authenticated key exchange in two phases. A secure, authenticated communication channel is established in phase 1. In phase 2 Security Associations are negotiated on behalf of IPsec.

IKE negotiates the following attributes:

1. Encryption algorithm
2. Hash algorithm
3. Authentication method
4. Diffie-Hellman group

In addition, a pseudo-random function can be negotiated. The HMAC version of the hash algorithm is used if no pseudo-random function is negotiated.

Mandatory IKE algorithms, methods and groups are:

- DES in CBC mode
- MD5 and SHA-1
- Authentication using pre-shared keys
- Modular exponentiation group one (768-bit Diffie-Hellman key exchange)

IKE should also support Triple-DES [17] for encryption, Tiger for hash, the DSS [8] and RSA signatures, RSA public key authentication and modular exponentiation group two (1024-bit Diffie-Hellman key exchange).

The authentication can be based on pre-shared secret, digital signatures or public key encryption. The RSA or DSS digital signatures can be based on certificates. When using authentication based on public key encryption, the identities of the communicating parties are kept secret.

## **5.2 Virtual Private Network**

Virtual Private Network (VPN) is one big logical network that is composed of distributed local area networks. VPN can be distributed across public, insecure networks. The information in transit in the public network is encrypted and authenticated.

On the edge of each distributed local area network there is a VPN gateway. The VPN gateways establish tunnels to peer VPN gateways on different local area networks. The VPN tunnels are IPsec connections in tunnel mode. Outbound IP packets to a network behind another VPN gateway are sent to the tunnel between the two gateways.

Virtual Private Network is seamless and transparent to users and applications. VPN operates on background after configuring.

## 5.3 Public Key Infrastructure

A standardised Public Key Infrastructure (PKI) for the Internet is specified in Internet X.509 Public Key Infrastructure Certificate and CRL Profile [13].

The users of the Internet PKI are people and processes that use client software. The users are the subjects of the certificates. The goal of the Internet PKI is to provide identification, authentication, access control and authorisation functions that are deterministic and automated.

### 5.3.1 X.509 Certificates

The purpose of certificate is to bind a public key to a subject and to assure that the associated private key is owned by the subject. The binding is asserted by having a trusted Certification Authority (CA) to sign the certificates. The CA can base the assertion upon technical means (proof of possession of the private key through challenge-response exchange), presentation of the private key or the assertion of the subject.

X.509 has specified a standard certificate format [16]. The first version (v1) was published 1988 as part of the X.500 Directory recommendations. In 1993 the X.500 was revised and two more fields were added. The result was version 2 (v2) format. The Internet Privacy Enhanced Mail (PEM) [18] RFCs was published in 1993. Experiences from the deployment of PEM pointed out that v1 and v2 X.509 certificates were deficient. In June 1996 the standardisation of version 3 (v3) X.509 certificates was completed.

The X.509 version 3 certificate mandatory fields are:

1. Version
2. Serial number
3. Issuer name
4. Validity period

5. Subject name
6. Subject's public key
7. Signature

The version can be v1, v2 or v3. The serial number must be unique for each certificate issued by a single Certification Authority. The issuer name and subject name are X.500 distinguished names (DN). Validity period is defined by the date on which the validity period begins and the date on which the validity period ends. The subject's public key contains an algorithm identifier and the public key bit string. The signature contains an algorithm identifier and the signature bit string.

The Internet PKI specifies standard extensions for the X.509 v3 certificates:

- Authority Key Identifier – the private key corresponding to the subject's public key is used to sign certificates.
- Key Usage – define the purpose of the key contained in the certificate (digital signature, non-repudiation, key encryption, data encryption, key exchange, certificate signature verification and CRL signature verification).
- Certificate Policies – indicates the Certification Practice Statement under which the certificate is issued.
- Policy Mappings – the issuer considers its domain policy equivalent to the subject CA's domain policy.
- Subject Alternative Name and Issuer Alternative Name – allows binding of additional identities to the subject and issuer (e.g. e-mail address, DNS name, IP address, uniform resource identifier (URI)).
- CRL Distribution Points – specifies an URI where the most current CRL can be found.

## **Revocation**

When certificate is issued, it is expected to be in use for the whole validity period. Circumstances that may cause the certificate to become invalid may arise before the end of the validity period. Examples of such situations are change of name, change of the association between the issuer and the subject (e.g. termination of employment within an organisation) and suspected compromise of the private key. Under these situations the certificates are revoked when an authorised person advises the CA of the abnormal situation.

X.509 defines one method for certificate revocation. CA periodically issues Certificate Revocation List (CRL), a signed list of revoked certificates. The CRL is freely available from a public repository (e.g. LDAP, HTTP, FTP or X.500).

The X.509 version 2 Certificate Revocation List contains the following fields:

1. Version
2. Issuer name
3. Date
4. Certificate serial numbers
5. Revocation dates

The CRL may also contain the date of next CRL update and extensions. Standard extensions include the reason why the certificate is revoked and instructions what to do if a revoked certificate is encountered.

### **5.3.2 Certificate Authority**

Certification Authority (CA) generates a certificate policy that it obeys when issuing certificates. The certificate policy should be reviewed before relying on the authentication and non-repudiation services based on certificates. The Internet PKI specification does not describe any legally binding rules or duties.

### 5.3.3 Certificate Validation

Certificate validation is verifying the binding between subject's distinguished name and/or alternative names and subject's public key.

A security service that requires a public key generally requires obtaining and validating the certificate that contains the public key. If an assured copy of the public key of the Certification Authority (CA) that has signed the certificate is not present, then an additional certificate must be obtained and validated. In complex systems a sequence of certificates must be obtained and verified.

The certificate path validation begins from a trusted CA. CA creates a self-signed certificate for itself. Trusted CA is defined in a system by storing the self-signed certificate in advance.

The certificate path validation is initialised with five state variables:

1. The certificate policy may be constrained to an acceptable policy set.
2. The certificate validation path namespace may be constrained to a subtree.
3. The certificate validation path namespace may exclude a subtree.
4. The certificate path validation may explicitly require a certificate policy.
5. The certificate path validation may allow certificate policy mapping.

The certificate path is validated by performing the following steps for each certificate starting from the self-signed certificate ending to the end-entity certificate:

1. Verifying that the certificate is valid:
  - a. The certificate was signed by the subject's public key from the previous certificate.
  - b. The certificate validity period includes current time.
  - c. The certificate is not revoked.
  - d. The issuer of the certificate is the subject of the previous certificate.

2. Verify that the subject name is in the constrained namespace subtree.
3. Verify that the subject name is not in the excluded namespace subtree.
4. Verify that the explicit policy requirement is met.
5. Verify that the acceptable policy set is

## 5.4 LDAP Directory

Lightweight Directory Access Protocol (LDAP) provides access to directories that support the X.500 models. LDAP is a lightweight subset of the DAP protocol in X.500 model. LDAP directory is a server that accepts requests from clients, processes them and sends responses back to the clients. In version 3 of the LDAP protocol the server can give references to other LDAP servers where to find the information, thus improving the performance and distribution. [43]

The LDAP data model is a Directory Information Tree (DIT), which can be accessed through one or more LDAP servers. The tree consists of entries. The entries have names. The name is made up of one or more attribute values of the entry. The name is called Relative Distinguished Name (RDN). RDN must be unique among all its siblings.

Schema is a collection of object class definitions, attribute type definitions and other information that helps the LDAP server to compare entries and control access. The object class attribute combined with the schema defines the allowed attributes for a given entry.

## 5.5 Secure DNS

Domain Name System (DNS) security extensions provide data integrity and authentication security services for Resource Records (RR), storage of public keys in special KEY RRs and optional transaction and request security.

The KEY RR associates public keys with DNS names. Secure DNS public key distribution mechanism can be used to secure the DNS protocol as well as other protocols.

## 6. Products

The reference system described in Chapter 7 is built from existing products. This chapter examines the available commercial products and chooses the products used in the following chapter.

### 6.1 Product Categories

There are several ways of creating an authentication framework for extranets. A solution that is built on Virtual Private Network (VPN), Certificate Authority (CA) and Lightweight Directory Access Protocol (LDAP) technologies is chosen because they have the best commercial availability.

To ensure interoperability, all commercially available products are based on standards. The technical features of all products are mainly dictated by the standards. Some products deliberately omit some features that are not commercially necessary, however. Other products add additional features not required by the standards to enhance the functionality of the product.

The differences between commercially available products are in the implementation, management, technical support and price. Different products have implementations on different hardware and operating system platforms. Each vendor has own management interface, more or less centralised. Technical support varies largely based on the local partners and sales channels. Price is always a big differentiator; some systems are targeted to low-end, entry environments and others to high-end, big enterprise environments.

#### 6.1.1 Virtual Private Network

All commercially available Virtual Private Network (VPN) products are based on the IPsec [21] and IKE [12] standards.

Mandatory features specified in IPsec and IKE are: DES encryption, MD5 and SHA-1 message authentication and authentication using pre-shared keys and 768-bit Diffie-Hellman key exchange. Mandatory features are implemented in every product if not stated otherwise.

### **CheckPoint FW-1/VPN-1**

CheckPoint FW-1/VPN-1 [3] is perhaps the most common commercially available firewall/VPN gateway.

Supported operating systems are Microsoft Windows NT 4.0 Service Pack 6 and earlier, Sun Solaris 2.6 and 7 (32-bit mode only), Red Hat Linux 6.0 and 6.1, HP-UX 10.20 and 11.0 (32-bit mode only) and IBM AIX 4.2.1 and 4.3.2.

CheckPoint FW-1/VPN-1 4.1 additionally supports 3DES, 40-bit DES, CAST, 40-bit CAST, FWZ-1 (proprietary 48-bit cipher) and 40-bit RC4 encryption algorithms. Additional asymmetric algorithms are 512-bit and 1024-bit RSA and 512-bit and 1024-bit Diffie-Hellman key exchange. Additional key exchange protocols are SKIP and FWZ (proprietary).

CheckPoint FW-1/VPN-1 has a high availability module that ensures smooth operation even in the case of hardware failure. The high availability is implemented with a two or more firewall/VPN gateway computer cluster. Also Stonesoft StoneBeat FullCluster clustering software can be used.

### **PGP Gauntlet Firewall/VPN**

PGP Gauntlet Firewall/VPN [33] is widely used commercial firewall/VPN gateway. Supported operating systems are Sun Solaris 2.6 and HP-UX 10.20.

PGP Gauntlet Firewall/VPN 6.0 additionally supports 3DES and CAST encryption algorithms. Additional asymmetric algorithms are 1024-bit and 1536-bit Diffie-Hellman key exchange.

PGP Gauntlet Firewall/VPN can be set up in high availability configuration that ensures smooth operation even in the case of hardware failure. The high availability is implemented with a two or more firewall/VPN gateway computer cluster using Legato Cluster Enterprise or Stonesoft StoneBeat FullCluster software.

### **Symantec Enterprise Firewall/VPN**

Symantec Enterprise Firewall [40] was formerly known as Raptor Firewall. Symantec Enterprise VPN was formerly known as PowerVPN. Symantec Enterprise Firewall/VPN is widely used commercial firewall/VPN gateway.

Supported operating systems are Microsoft Windows NT 4.0, Microsoft Windows 2000 and Sun Solaris 2.6 and 7.

Symantec Enterprise Firewall/VPN 6.5 additionally supports 3DES encryption algorithm. Additional asymmetric algorithm is 1024-bit Diffie-Hellman key exchange.

Symantec Enterprise Firewall/VPN can be set up in high availability configuration that ensures smooth operation even in the case of hardware failure. The high availability is implemented with a two or more firewall/VPN gateway computer cluster using Microsoft Cluster Server or Stonesoft StoneBeat FullCluster software.

### **F-Secure VPN+**

F-Secure VPN+ [11] is a stand-alone VPN gateway. Supported operating systems are Microsoft Windows 95/98, Microsoft Windows NT 4.0 and Linux. Microsoft Windows 2000 and Sun Solaris are supported in a future release.

F-Secure VPN+ 5.0 additionally supports 3DES, CAST and Blowfish encryption algorithms. Additional asymmetric algorithm is 1024-bit RSA key exchange.

F-Secure VPN+ 5.0 also contains F-Secure Certificate Wizard that can be used to create certificates for the VPN gateways. F-Secure Certificate Wizard can be used as a lightweight CA.

## **Stonesoft StoneGate**

Stonesoft StoneGate [39] is a new firewall/VPN gateway that has been developed from the start as a high availability solution. Stonesoft StoneGate runs on a hardened Linux operating system. The management software can be run on Microsoft Windows NT 4.0, Microsoft Windows 2000, Linux and Sun Solaris.

## **IBM SecureWay Firewall/VPN**

IBM security products are based on Tivoli Enterprise Architecture. The Tivoli Enterprise Architecture is a comprehensive security framework targeted to large enterprises.

IBM SecureWay Firewall/VPN [42] is a firewall/VPN gateway product that is based on the Tivoli Enterprise Architecture. Supported operating system is AIX 4.3.2 and later.

IBM SecureWay Firewall/VPN 4.1 additionally supports 3DES encryption algorithm. It does not support IKE so the VPN tunnels must be created manually using IPsec SAs.

## **FreeS/WAN**

FreeS/WAN [10] is an open-source VPN gateway. Supported operating system is Linux operating system kernels 2.0, 2.2 and 2.4.

FreeS/WAN 1.9 does not support DES or 768-bit Diffie-Hellman key exchange because they are considered insecure. Instead, FreeS/WAN supports 3DES, 1024-bit and 1536-bit Diffie-Hellman key exchange. FreeS/WAN supports Secure DNS. Additionally patches that add support for X.509 certificates, Blowfish, IDEA and CAST are available.

### **6.1.2 Certificate Authority**

All commercially available Certificate Authority (CA) products are based on X.509 [16] and LDAP [43] standards.

Most vendors integrate other vendor products together with their own firewall or other security product to create a CA.

### **CheckPoint Certificate Manager**

CheckPoint Certificate Manager [2] is a turnkey PKI solution. It is integrated from CheckPoint Account Management Client, Entrust Certificate Authority and Netscape Directory Server. Supported operating system is Microsoft Windows NT 4.0 Service Pack 3 or later.

The CheckPoint Certificate Manager only integrates other well-known products with CheckPoint FW-1/VPN-1. Tight integration ensures interoperability and smooth operation.

### **RSA Keon Sentry CA**

RSA Keon Sentry CA [34] is a lightweight Certification Authority. RSA Keon Sentry CA was originally made by Xcert. RSA bought Xcert in 2001. Supported operating systems are Microsoft Windows NT 4.0 Service Pack 4 or later, Microsoft Windows 2000 Service Pack 1 or later and Sun Solaris 2.6 or 7.

RSA Keon Sentry CA 4.7 has a web-based management and administration interface. It has built-in web server and LDAP server. It is designed for fault tolerance, load balancing and component redundancy to maintain performance in large systems.

RSA Keon Sentry CA 4.7 supports RSA, Digital Signature Algorithm (DSA) and Elliptic Curve (EC) public key technologies. Core benefit of Elliptic Curve public key technology against RSA is performance. 163-bit EC key is considered equivalent to 1024-bit RSA key.

RSA Keon Sentry CA 4.7 has built-in support for token and smart cards such as Luna CA line of tokens from Chrysalis-ITS and nCipher nForce.

## **RSA Keon Certificate Server**

RSA Keon Certificate Server [34] is a Certificate Authority made by RSA itself. RSA Keon Certificate Server 5.5.1 contains Netscape Enterprise Server and Netscape Directory Server. Supported operating systems are Microsoft Windows NT 4.0, Microsoft Windows 2000 and Sun Solaris.

RSA Keon Certificate Server is managed and administered through a web GUI. Netscape Enterprise Server provides the web interface. Netscape Directory Server is used as a LDAP server to store certificates and CRLs. Supported certificate formats are SSL, S/MIME, IPsec and PKIX. The RSA Keon Certificate Server CA can be partitioned into administrative domains using digital certificates.

## **Entrust PKI**

Entrust PKI [7] is a widely used Certification Authority, which is bundled in many third party products that require CA. Supported operating systems are Microsoft Windows NT 4.0, Sun Solaris 2.6 and 7, HP-UX 10.20 and 11.0 and IBM AIX 4.3.2 and 4.3.3.

Entrust PKI supports RSA, Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) for signing certificates. It supports DES, 3DES, CAST, RC2, RC4 and IDEA symmetric ciphers.

## **iPlanet Certificate Management System**

iPlanet Certificate Management System [14] is a part of the iPlanet suite, which was formerly known as Netscape suite. Supported operating systems are Compaq Tru64 4.0D, HP UX B.11.00, IBM AIX 4.3.3, Microsoft Windows NT 4.0 Service Pack 5 or later, Sun Solaris 2.6, 7 and 8.

iPlanet Certificate Management System 4.2 Service Pack 2 supports X.509v3 and wTLS-compliant certificates. Supported signing and encryption algorithms are 1024-4096-bit DSA and RSA. Supported hashing algorithms are MD2, MD5 and SHA-1.

Supported certificate request message formats are KEYGEN/SPAC, CRMF/CMMF, CRS/CEP/SCEP, PKCS #10 and CMC. Supported certificate formats are SSL, S/MIME, IPsec and Cisco.

Supported CRL formats are X.509 CRL v1 and v2. CRLs can be published by LDAP or HTTP/HTTPS to any LDAP compliant directory and as a flat file to Oracle RDBMS. iPlanet Certificate Management System supports online certificate verification by an OCSP responder.

iPlanet Certificate Management System includes four servers. Certificate Manager is the CA. Registration Manager can be used to delegate some functions to an RA. Data Recovery Manager provides key archival and recovery services. Online Certificate Status Manager is the OCSP responder.

### **6.1.3 LDAP Directory**

Commercially available LDAP directory servers are targeted for large, enterprise-wide systems. Smaller LDAP servers are many times integrated into the Certificate Authority itself.

#### **iPlanet Directory Server**

iPlanet Directory Server [15] was formerly known as Netscape Directory Server. iPlanet Directory Server is a powerful and scalable distributed directory server for large enterprises. Supported operating systems are Microsoft Windows NT 4.0 Server, Microsoft Windows 2000 Server, Sun Solaris 2.6 and 8 (32- and 64-bit), HP-UX 11.0 and IBM AIX 4.3.3.

iPlanet Directory Server 5.0 consists of an LDAP Server, Directory Server Console, Directory Server Gateway, iPlanet Directory Express, SNMP Agent and Online backup and restore.

LDAP Server is the core of the directory server. Directory Server Console is a part of iPlanet Console, the common management framework for iPlanet servers. Directory Server Gateway is a HTTP to LDAP client, which allows administration of the directory server using a web browser. iPlanet Directory Express is a simple LDAP lookup tool. SNMP Agent allows monitoring in real time using Simple Network Management Protocol (SNMP). Online backup and restore tool allows creation of backups and restoration from backups while the directory server is running.

### **IBM SecureWay Directory**

IBM SecureWay Directory [41] is a cross-platform, highly scalable and robust directory server for large enterprises. Supported operating systems are Microsoft Windows NT 4.0 Service Pack 4 or later, Sun Solaris 2.6 or 7 (32-bit only), IBM AIX 4.3.3, OS/390 and OS/400.

IBM SecureWay 3.2.1 supports SSL, Kerberos, access control, referrals, certificate management, client authentication, replication, LDAP browsing through HTTP, Simple Authentication and Security Layer (SASL), CRAM-MD5 authentication, change log, UserPassword encryption and UTF-8 databases.

## **6.2 Virtual Private Network Evaluation**

Four Virtual Private Network products are chosen for comparison. The products that support Sun Solaris operating system are evaluated. The reason for Sun Solaris support requirement is that in the telecommunications field Sun Solaris is regarded as the most reliable platform. Exception to the requirement for Sun Solaris support is FreeS/WAN, it is chosen for closer look because it is open source and thus free.

### **6.2.1 CheckPoint FW-1/VPN-1**

CheckPoint FW-1/VPN-1 supports 3DES and SHA-1 so the IPsec connections can be considered secure. It also supports CAST symmetric cipher, RSA asymmetric cipher, SKIP key management protocol and Perfect Forward Secrecy (PFS).

Supported key exchange algorithms are 1024-bit RSA and 1024-bit Diffie-Hellman.

Supported end entity authentication methods are RADIUS, TACACS/TACACS+, token-based (two factor), operating system password, FireWall-1 password, S/KEY seed-based one-time passwords and digital certificates.

### **6.2.2 PGP Gauntlet Firewall/VPN**

PGP Gauntlet Firewall/VPN supports 3DES and SHA-1 so the IPsec connections can be considered secure. It also supports CAST symmetric cipher, IP compression and Perfect Forward Secrecy (PFS).

Supported key exchange algorithms are 1024-bit and 1536-bit Diffie-Hellman.

Supported end entity authentication methods are RADIUS, CryptoCard, Defender Security Server, password, SecurID, SecureNet Key and S/KEY seed-based one-time passwords and digital certificates.

### **6.2.3 Symantec Enterprise Firewall/VPN**

Symantec Enterprise Firewall/VPN supports 3DES and SHA-1 so the IPsec connections can be considered secure. It does not support Perfect Forward Secrecy (PFS), however.

Supported key exchange algorithm is 1024-bit Diffie-Hellman.

Supported end entity authentication method is RaptorMobile, Symantec's own VPN client.

### **6.2.4 FreeS/WAN**

FreeS/WAN supports 3DES and SHA-1 so the IPsec connections can be considered secure. It additionally supports IP compression and Perfect Forward Secrecy (PFS). Blowfish, IDEA and CAST symmetric ciphers are also supported as patches.

Supported key exchange algorithms are 1024-bit and 1536-bit Diffie-Hellman.

Supported end entity authentication methods are Secure DNS and X.509 digital certificates.

## 6.2.5 Virtual Private Network Feature Matrix

The main features of Virtual Private Networks are presented in Table 1 below.

*Table 1. VPN feature matrix.*

	ESP			AH		IPsec	Asymmetric		Key Exchange		
	D E S	C A T	3 D E S	M D 5	S H A - 1		R S A	Diffie- Hellman	I K E	S K I P	P F S
CheckPoint FW-1/VPN-1	✗	✗	✗	✗	✗		✗	✗	✗	✗	✗
PGP Gauntlet Firewall/VPN	✗	✗	✗	✗	✗	✗		✗	✗		✗
Symantec Enterprise Firewall/VPN	✗		✗	✗	✗			✗	✗		
FreeS/WAN			✗	✗	✗	✗		✗	✗		✗

CheckPoint FW-1/VPN-1 is chosen because it has the best algorithm and protocol support. It also has the largest market share and thus easily justified to teleoperators. Only downside is the cost. FreeS/WAN would meet most of the needs and does not cost anything. But open source software is not considered very reliable in the telecommunications field.

## 6.3 Certificate Authority Evaluation

Three Certificate Authority products are chosen for comparison.

### **6.3.1 CheckPoint Certificate Manager**

CheckPoint Certificate Manager is chosen for comparison because of its tight integration with CheckPoint FW-1/VPN-1. It has quite extensive feature list because it includes industry-leading Entrust CA and Netscape Directory Server.

CheckPoint Certificate Manager is quite expensive, however. It is also quite heavy system only to authenticate VPN gateways. The Entrust CA and Netscape Directory Server products can be used to create large systems containing millions of end entities.

### **6.3.2 RSA Keon Sentry CA**

RSA Keon Sentry CA is a compact, complete CA solution, which contains a web-based CA and integrated LDAP server. The price is also quite affordable.

Easy deployment and support for smart cards and elliptic curve public key cryptosystem are the benefits of RSA Keon Sentry CA.

### **6.3.3 iPlanet Certificate Management System**

iPlanet Certificate Management System is even more feature-rich than the CheckPoint Certificate Manager. It is a multi-purpose, large-scale system for millions of end entities. The calibre of the end entity number and price make it infeasible for only VPN gateway authentication.

### **6.3.4 Certificate Authority Feature Matrix**

The main features of Certificate Authorities are presented in Table 2 on page 52.

**Table 2.** Certificate Authority feature matrix.

	GUI	LDAP server	RSA	DSA	EC
CheckPoint Certificate Manager	Own	External	✍	✍	✍
RSA Keon Sentry CA	Web	External	✍	✍	✍
iPlanet Certificate Management System	Web & Own	Integrated	✍	✍	✍

RSA Keon Sentry CA is chosen because of the easy deployment and affordable price. Despite the fact that RSA Keon Sentry CA is compact and affordable, the list of features is complete. Only features regarding division into administrative domains and distribution are not supported as extensively.

## 6.4 LDAP Directory Evaluation

Both LDAP directories are chosen for comparison in addition to the integrated LDAP server of the RSA Keon Sentry CA.

### 6.4.1 RSA Keon Sentry CA

The LDAP server of RSA Keon Sentry CA supports all the necessary features such as access control, backup and recovery and publishing to external LDAP server.

### 6.4.2 iPlanet Directory Server

iPlanet Directory Server is intended for e-commerce sites containing web servers, certificate authorities and LDAP servers. All these products can be found from the iPlanet product suite. The interoperability of iPlanet suite products works very well.

For VPN gateway authentication purposes iPlanet Directory Server is too massive.

### 6.4.3 IBM SecureWay Directory

IBM SecureWay Directory is intended for all kinds of large information systems that can be distributed globally and administered centrally. Tivoli Enterprise Architecture is a comprehensive management framework. Administration of large systems is made as easy as possible.

For VPN gateway authentication purposes IBM SecureWay Directory is too massive.

### 6.4.4 LDAP Directory Feature Matrix

The main features of LDAP Directories are presented in Table 3 below.

*Table 3. LDAP Directory feature matrix.*

	Deployment	Scalability	Management
RSA Keon Sentry CA	Easy	Limited	Limited centralisation
iPlanet Directory Server	Fairly easy	Good	Centralised
IBM SecureWay Directory	Fairly easy	Very good	Centralised

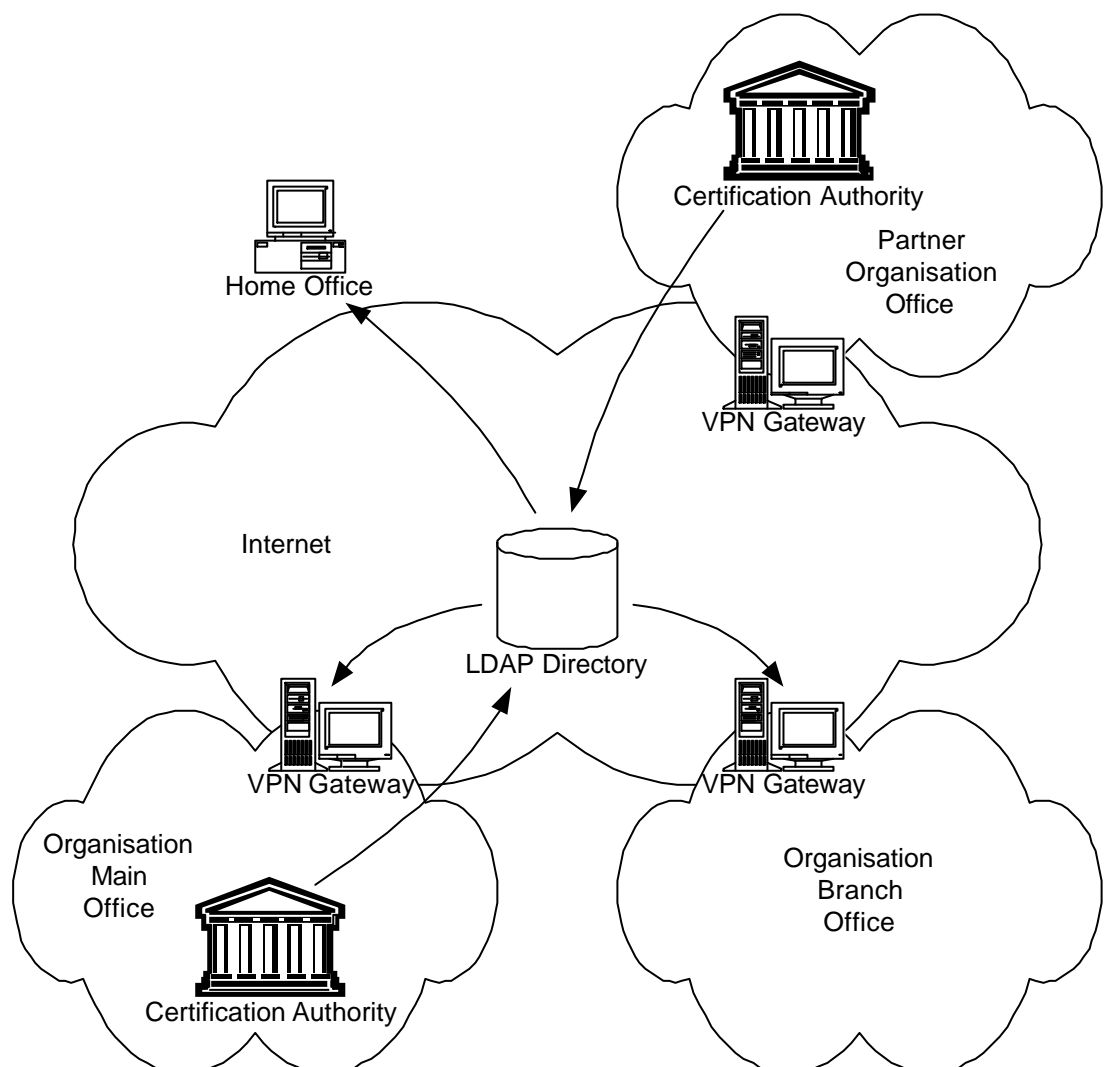
RSA Keon Sentry CA is chosen because of the easy deployment and affordable price. It is best suited for small- or medium-sized systems.

# 7. Reference System

One of the main goals of this thesis is to build a reference system that fulfils the criteria defined in Chapter 3.

## 7.1 Architecture

The reference system architecture is illustrated in Figure 10 below.



*Figure 10. Reference system architecture.*

The organisation has a main office and a branch office. Both offices have their own VPN gateway. The VPN gateway is on the edge between the organisation network and the Internet. The organisation also has a Certification Authority, which is located in the main office.

LDAP directory is publicly available in the Internet. The Certification Authority puts certificates to the LDAP directory. The VPN gateways and the home office get certificates from the LDAP directory.

Partner organisation also has an office that is connected to the Internet. The partner organisation office also has a VPN gateway and a Certification Authority. The partner organisation Certification Authority also puts certificates to the same LDAP directory. The partner organisation VPN gateway also gets certificates from the same LDAP directory.

## **7.2 VPN Gateway**

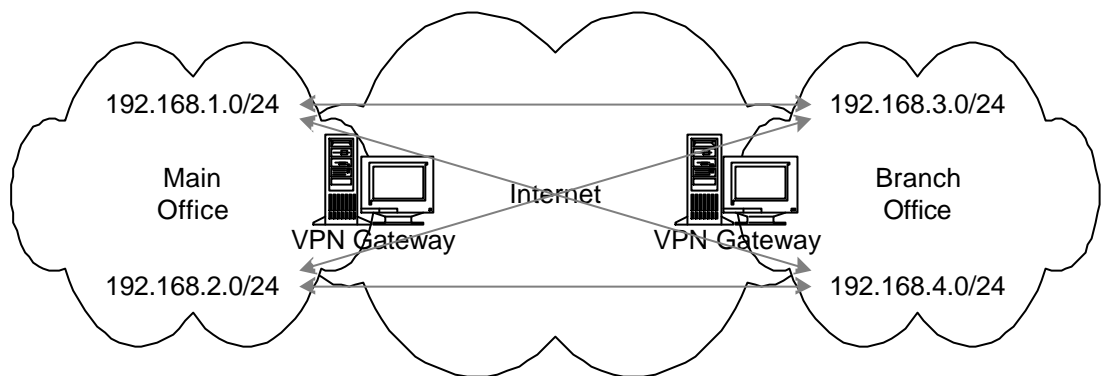
The VPN gateway is implemented on a Sun workstation running a Solaris operating system. The VPN software is an integrated firewall and VPN gateway from CheckPoint. The specifications of the VPN gateway can be found from Appendix A.

Each VPN gateway is assigned an encryption domain. The encryption domain contains IP addresses that can be found behind the VPN gateway. The encryption domain is defined by a group of IP address and netmask pairs.

The VPN gateway also has the knowledge of all other VPN gateways and their respective encryption domains. VPN gateway is like a router, which forwards IP packets. Special care is given to IP packets which source IP address is within the local VPN gateway's encryption domain and destination IP address is within the encryption domain of another known VPN gateway. They are forwarded to an IPsec tunnel between the VPN gateways that provide encryption and authentication security services.

The IPsec tunnel is established only when needed. It is established when a packet is received and is kept alive for few minutes for any subsequent packets that may arrive and have the same destination. An IPsec tunnels is bi-directional so reply packets can use the already existing IPsec tunnel.

There is a separate IPsec tunnel for every IP network address pair even if the IPsec tunnel endpoints are the same. For example if organisation's main office consists of IP networks 192.168.1.0/24 and 192.168.2.0/24 and branch office 192.168.3.0/24 and 192.168.4.0/24, then there would be four IPsec tunnels (See Figure 11 below).



*Figure 11. Example of possible IPsec tunnels between two VPN gateways.*

## 7.3 Certificate Authority

The Certification Authority (CA) is implemented on a Windows NT PC. The CA software is an integrated CA and LDAP directory from RSA. The specifications of the CA can be found from Appendix A.

The RSA Keon Sentry CA is administered by using HTTP protocol. There are four different HTTP servers: administration server, enrollment server, Simple Certificate Enrollment Protocol (SCEP) server and Certificate Revocation List (CRL) server. All HTTP servers have their own SSL server certificate to verify the identity of the server and to encrypt the communications. The SSL server certificates are issued by the Sentry CA.

### **7.3.1 Administration Server**

The administration server is a web based GUI for carrying out administrative tasks such as issuing, suspending, reinstating and revoking certificates for end-entities, issuing, suspending, reinstating and revoking certificates for sub-CAs, publishing CRLs and configuring the CA software.

In addition to the server authentication the administration server also uses certificate-based client authentication. During installation an administration certificate is issued and stored in the administrator's web browser. Also the corresponding private key is stored in the administrator's web browser. The administration certificate and corresponding private key can be copied to authorised persons. Only persons, who possess the administration certificate's private key, can administer the CA.

### **7.3.2 Enrollment Server**

The enrollment server is a web based GUI for typing in certificate requests. The certificate requests use the PKCS #10 [31] format. The certificate request form can also be filled in by hand.

The certificate requests are then handled in the administration console on the administration server. Notification of the issued certificate is sent by e-mail containing an URL where the actual certificate can be downloaded and taken into use.

### **7.3.3 SCEP Server**

The SCEP server is protocol on top of HTTP for certificate enrollment. SCEP [44] is a machine-to-machine interface specified by Cisco. The certificate requests can be handled in the same ways as with the enrollment server or automatically based on a configured set of rules.

### **7.3.4 CRL Server**

The CRL server is an HTTP server for CRL retrieval. CRL can be generated manually or Sentry CA can be configured to generate a CRL periodically or automatically after suspending, reinstating or revoking a certificate. CRL can also be published in LDAP directory (see below) instead of the HTTP server.

Sentry CA also provides another mechanism for revoked certificates verification. Online Certificate Status Protocol (OCSP) is an online mechanism for checking revocation of a certificate [29].

Manually or periodically published CRL has the weakness that it is inherently outdated information immediately after the CRL is published. The CRL has a validity period after which an updated CRL is published. In the mean time all the revoked certificates can still be used. The OCSP protocol does not have this problem. The certificate status is always checked when it is used. If a certificate is revoked, the change is immediately reflected in the entire PKI.

## **7.4 LDAP Directory**

RSA Keon Sentry CA contains an integrated LDAP directory, Secure Directory Server. The Secure Directory Server contains issued certificates and Certificate Revocation List (CRL).

The Sentry CA publishes issued certificates to the Secure Directory Server. Clients can then download certificates from the Secure Directory Server. CRL can be published manually, automatically when certificate is suspended, reinstated or revoked or periodically.

Sentry CA can also be used with an external LDAP directory. The internal LDAP directory can also be configured to receive certificates and CRLs from other CAs.

## 7.5 VPN Authentication

CheckPoint VPN-1 supports two authentication methods when using Internet Key Exchange (IKE): pre-shared secrets and X.509 digital certificates.

### 7.5.1 VPN Gateways

These two authentication methods are the only possibilities when connecting distributed local area networks together with VPN gateways. The computers inside the local area networks are transparently connected to each other.

### 7.5.2 VPN Clients

It is also possible to connect a computer outside the local area networks to the VPN network. Roadwarriors are mobile users that need to access the organisations network on the move. Also home offices can use the same mechanism.

The mobile computer requires a VPN client that makes the connection to a VPN gateway. The VPN client is a simple program that contains an IPsec protocol stack and administrative interface for configuring the VPN connections.

CheckPoint VPN-1 supports seven different end user authentication methods: S/KEY, SecurID, VPN-1 password, operating system password, RADIUS, AXENT Pathways Defender and TATACS.

As with the VPN gateways, X.509 digital certificates or IKE pre-shared secret are used to initiate the IKE key negotiation. The end user itself can then be authenticated using the password, seeded one-time passwords, smart card or other security device.

## 7.6 Trust Hierarchy

The reference system hierarchy is based on extensive use of X.509 digital certificates. The Certification Authority issues certificates to each VPN gateway and each roadwarrior end user. The VPN gateway certificates and corresponding private keys are delivered to the VPN system.

The end user certificates and corresponding private keys are given to the respective end users. The end users store the certificates and corresponding private keys in the hard disk of their computer.

### 7.6.1 VPN Gateways

When a VPN gateway tries to establish connection with another VPN gateway, the authenticity of the end points is based on either:

1. The verification of digital signatures generated by the private keys of the VPN gateway certificates or,
2. The ability of decrypt nonces encrypted with the public keys of the VPN gateway certificates.

The VPN gateways have established peer VPN gateways' certificates as trusted certificates in the VPN system configuration phase.

### 7.6.2 VPN Clients

When a VPN client tries to establish connection with a VPN gateway, the authenticity of the VPN client is based on the same mechanisms as with VPN gateways.

VPN client authentication has however another level of security: The end user authentication is based on something known (i.e. password), something possessed (i.e. smart card) or any combination of these.

The trust of a VPN client is established by the fact that the authorised end user has only the knowledge or possession of the required authentication token.

# 8. Analysis

This chapter gives an analysis of the reference system described in Chapter 7 against the criteria specified in Chapter 3.

## 8.1 Criteria

**Criterion 1** The algorithms must use strong cryptography.

The specifications for cryptographic algorithms are public (3DES [17], HMAC-SHA-1-96 [27] and RSA [36]). The algorithms are also very widely used and have no known weaknesses.

**Criterion 2** The algorithms must use strong keys.

The reference system uses 3DES for symmetric encryption, SHA-1-96 for keyed Hash Message Authentication Code (HMAC) and 1024-bit RSA keys for asymmetric encryption.

The best known attack against 3DES requires  $2^2$  known plaintext-ciphertext pairs,  $2^{112}$  encryptions and requires  $2^{56}$  words of memory. [22]

HMAC-SHA-1-96 uses 96-bit key and has no known weaknesses [24]. HMAC-MD5-96 has been shown to be vulnerable to collision search attack [5] and is not used in the reference system.

The complexity a brute force attack against 1024-bit RSA asymmetric key is equivalent to 96-bit symmetric key (effective key length of 3DES is 112 bits). Estimated time to break 96-bit symmetric key or 1 024-bit asymmetric key using brute force attack is 3 000 000 years. [37]

Recommended effective key length for symmetric algorithms is 96 bits and 1024 bits for asymmetric algorithms, just to be sure. The increase of key length has linear effect to the performance of the algorithm but exponential effect to the security.

Thus 3DES, HMAC-SHA-1-96 and 1024-bit RSA are considered strong cryptographic algorithms.

**Criterion 3** The protocol must implement Virtual Private Network at IP-level.

VPN is based on IPsec standards that provide the security services at the IP level. The VPN is completely transparent to users after it is built. [21]

**Criterion 4** No plaintext authentication tokens (passwords etc.) must pass across insecure networks.

Authentication is based on public keys using X.509 digital certificates. No private keys or secret keys are sent to the network unprotected. [12]

Secret keys may be used in VPN client authentication, but in that case the connection is already secured with IPsec using X.509 digital certificate.

**Criterion 5** The protocol must provide confidentiality, integrity and protection against replay attacks.

IPsec Encapsulating Security Payload (ESP) is used to provide confidentiality using symmetric encryption with a session key, which is generated when establishing the Security Association (SA). [20]

IPsec Authentication Header (AH) is used to provide integrity and protection against replay attacks using keyed Hash Message Authentication Code and Sequence Number. [19]

**Criterion 6** The protocol must provide authenticated keying material that is kept confidential.

Internet Security Association and Key Management Protocol (ISAKMP) provide authenticated confidential keying material using random nonces and public key encryption. [28]

**Criterion 7** The complexity of key management must be at most linear as the number of parties increase.

Each VPN gateway and each end user require one certificate. Thus the complexity of key management grows linearly.

If pre-shared secrets would be used, each pair of end points would need its own secret key. The number of pre-shared secrets would grow exponential as the number of end points increase. Pre-shared secrets is not a feasible authentication method in large systems.

**Criterion 8** The protocol must provide Perfect Forward Secrecy.

Internet Key Exchange (IKE) provides Perfect Forward Secrecy (PFS) for both the keying material and the identities.

PFS for keying material is established by specifying a Diffie-Hellman group and passing public key values in the key exchange payload. PFS for identities is established by using encryption keying material in the ISAKMP SA. [12]

**Criterion 9** The administrator of a network must be able to decide which partner networks are permitted access.

Access control is achieved by defining specific rules for different partner organisations and different local area network combinations. The CheckPoint VPN-1 administration GUI has an easy-to-use interface to perform this task.

**Criterion 10** The system must be built using already existing products.

CheckPoint VPN-1 is a commercial product from CheckPoint Software Technologies Ltd. CheckPoint VPN-1 was introduced several years ago and is widely used.

RSA Keon Sentry CA is a commercial product from RSA Security. Sentry CA was developed by Xcert Software, which was purchased by RSA Security in 2001. Xcert Software was founded in 1996. Sentry CA was introduced several years ago and is also widely used.

## **8.2 Authentication Model**

The authentication in the VPN gateways is based on certificates. In addition to the possession of certificate, the name of the subject of the certificate must be the same as the name of the end point computer.

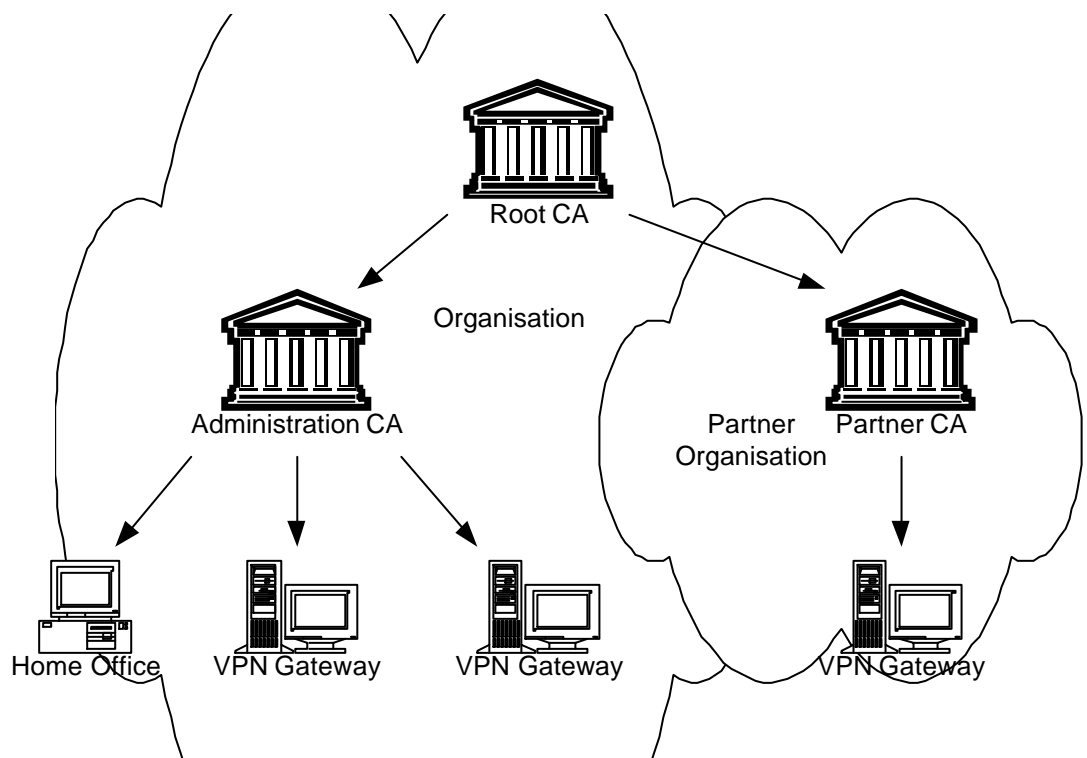
If the authentication is based on the possession of a private key that corresponds to a certificate there is always the threat of private key exposure. In VPN gateways the possibility of private key exposure is not very high. The VPN gateways are machines that do not require network logins or any other software that would introduce possible backdoors.

In VPN clients the threat of private key exposure is much more probable to happen. Somebody can break into a home office or a laptop belonging to a road warrior can be stolen. This is the reason why the VPN client authentication has an additional level of security. The access to the organisation's network can be protected with additional username and password or a physical security device such as a smart card.

The authentication method is evaluated to be secure under the assumption that good security practices are followed when installing certificates and corresponding private keys corresponding and choosing passwords.

### 8.3 Trust Model

At the root of the trust hierarchy there is a single Root Certification Authority (CA). Root CA is trusted by everyone. The Root CA delegates the right to issue certificates to sub-CAs. There is one sub-CA for the organisation's own use, the Administration CA and one sub-CA for each partner organisation (see Figure 12 below for illustration).



*Figure 12. Certificate Authority hierarchy.*

The VPN administrator can now grant access rights for each VPN gateway and VPN client. The certificate for every end point can be retrieved from the LDAP directory and input to the system.

The CAs asserts the identities of the end points but the VPN administrator can grant the access rights.

## **8.4 Business World**

Despite the excellence of technology, business issues may arise that prevent the introduction of the authentication mechanism. Does the partner organisation actually trust the Certification Authority?

The business world is mainly concerned with contractual and financial issues. These issues are out of the scope of this thesis and are not explored in more detail.

## 9. Conclusions

Extranet that is based on IPsec VPN technology are in many ways a good solution. IPsec is a widely adopted standard, which has also been proved in practice. There are many software vendors that have IPsec compliant VPN gateways and VPN client software. The support covers a wide range of platforms and operating systems. In most cases there is even freedom of choice between similar products so that the product matches the organisation's individual preferences best.

Authentication that is based on digital certificates is in many ways superior to authentication that is based on secrets. Key management is much easier because the authentication tokens are public and no secret information is required to be exchanged before establishing a connection. In addition to easier key management, it is also very much easier to grant access permissions across organisational boundaries.

The reference system described in this thesis uses IPsec VPN for creating extranets and digital certificates for authentication. The reference system fulfils all of the criteria specified for a useful system. Additionally the reference system also includes an easy approach to build the desired trust model between organisations.

### 9.1 Tecnomen Maintenance Connections

The reference system can be used to make maintenance connections from Tecnomen's central site to customer locations all over the world. Especially the trust model is flexible and easy to change access permissions. Only minimal administration work is required at the customer site when access permissions change.

The conclusion of this thesis is a proposition to take the reference system into use for remote maintenance connections.

## **9.2 Future Work**

The network security field is developing fast and new and better algorithms and protocols are specified. This section gives some pointers where to look in the future as of summer 2001.

### **9.2.1 Advanced Encryption Standard**

The successor of Data Encryption Standard (DES), Advanced Encryption Standard (AES) [30] has been published for public review in February 2001. If the AES development process proceeds as planned, the standard will be completed by the summer of 2001.

### **9.2.2 Smart Cards**

Smart cards have been used for authentication purposes for some time. The problem with smart cards and other security devices is that they are vendor-specific proprietary solutions. Thus they are not yet adopted in large, open systems where all kinds of different platforms and different needs can be found.

Fortunately, there are emerging smart card standards that utilise open, widely adopted mechanisms. Examples of such emerging systems are SecurID smart cards [35] containing X.509 digital certificates and Subscriber Identity Modules (SIMs) containing public and private key cryptography [38].

### **9.2.3 FreeS/WAN**

FreeS/WAN [10] is an open source implementation of a VPN gateway and client. As open source it helps the adoption of VPN technology in a wide range of new areas.

Open source development has some inherent advantages. Perhaps the most important is that it is secure in a way that there can be no hidden backdoors because the source code is public and anyone can build the binaries by themselves in their own trusted development environment. Additionally, because the source code is public, it has received valuable public review discovering bugs that could cause security breaches.

The development of open source products is also rapid because a large number of developers can participate in the development effort. It can be seen for example from the Linux operating system that open source fosters rapid development.

FreeS/WAN already have some leading-edge features such as support for Secure DNS [6] and opportunistic encryption. This is a direct result from the benefits of open source development.

Security software is also often expensive. Open source implementations can be acquired and used for free.

#### **9.2.4 Biometrics**

Security devices that use biometrics as an authentication mechanism, are currently either too expensive or too unreliable. The development of biometrics security devices is however rapid and in the future we can log on to a computer by fingerprint, retina scan, voice identification or signature. It will be interesting to follow the development in the biometrics field.

# References

- [1] Amoroso, E., Fundamentals of Computer Security Technology, Prentice Hall, New Jersey, 1994, 404 p.
- [2] CheckPoint, VPN-1 Certificate Manager, 6.6.2001, [referred 27.6.2001]  
<<http://www.checkpoint.com/products/vpn1/certificate.html>>
- [3] CheckPoint, VPN-1 Product Family, 28.5.2001, [referred 27.6.2001]  
<<http://www.checkpoint.com/products/vpn1/index.html>>
- [4] Dierks, T. & Allen, C., The TLS Protocol Version 1.0, January 1999, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2246.txt>>
- [5] Dobbertin, H., The Status of MD5 After a Recent Attack, RSA Laboratories' CryptoBytes, Vol. 2 No. 2, Summer 1996, [referred 27.6.2001]  
<<ftp://ftp.rsasecurity.com/pub/cryptobytes/crypto2n2.pdf>>
- [6] Eastlake, D., Domain Name System Security Extensions, March 1999, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2535.txt>>
- [7] Entrust, Entrust/PKI, 6.5.2001, [referred 27.6.2001]  
<<http://www.entrust.com/entrust/index.htm>>
- [8] Federal Information Process Standards, Digital Signature Standard (DSS), U.S. Department of Commerce, National Institute of Standards and Technology, 27.1.2000 [referred 27.6.2001]  
<<http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf>>
- [9] Free On-Line Dictionary Of Computing, [referred 27.6.2001]  
<<http://foldoc.doc.ic.ac.uk/foldoc/>>

- [10] FreeS/WAN, [referred 27.6.2001]  
<<http://www.freeswan.org/>>
- [11] F-Secure, F-Secure VPN+, [referred 27.6.2001]  
<<http://www.f-secure.com/products/vpnplus/>>
- [12] Harkins, D. & Carrel, D., Internet Key Exchange (IKE), November 1998, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2409.txt>>
- [13] Housley, R. & Ford, W. & Polk, W. & Solo, D., Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, January 1999, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2459.txt>>
- [14] iPlanet, iPlanet Certificate Management System, [referred 27.6.2001]  
<[http://www.ipplanet.com/products/ipplanet\\_certificate/home\\_2\\_1\\_1ad.html](http://www.ipplanet.com/products/ipplanet_certificate/home_2_1_1ad.html)>
- [15] iPlanet, iPlanet Directory Server, [referred 27.6.2001]  
<[http://www.ipplanet.com/products/ipplanet\\_directory/home\\_2\\_1\\_1z.html](http://www.ipplanet.com/products/ipplanet_directory/home_2_1_1z.html)>
- [16] ITU-T, Recommendation X.509 (1997 E): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, June 1997
- [17] Karn, P. & Metzger, P. & Simpson, W., The ESP Triple DES Transform, September 1995, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc1851.txt>>
- [18] Kent, S., Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, February 1993, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc1422.txt>>
- [19] Kent, S. & Atkinson, R., IP Authentication Header, November 1998, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2402.txt>>

- [20] Kent, S. & Atkinson, R., IP Encapsulating Security Payload (ESP), November 1998, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2406.txt>>
- [21] Kent, S. & Atkinson, R., Security Architecture for the Internet Protocol, November 1998, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2401.txt>>
- [22] Knudsen, L. R. & Rijmen, V., The Block Cipher Lounge, 15.6.1998, [referred 27.6.2001]  
<<http://www.esat.kuleuven.ac.be/~rijmen/bc.html>>
- [23] Krawczyk, H., SKEME: A Versatile Secure Key Exchange Mechanism for Internet, IEEE Proceedings of the 1996 Symposium on Network and Distributed Systems Security
- [24] Krawczyk, H., & Bellare, M. & Canetti, R., HMAC: Keyed-Hashing for Message Authentication, February 1997, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2104.txt>>
- [25] Madson, C. & Doraswamy, N., The ESP DES-CBC Cipher Algorithm with Explicit IV, November 1998, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2405.txt>>
- [26] Madson, C. & Glenn, R., The Use of HMAC-MD5-96 within ESP and AH, November 1998, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2403.txt>>
- [27] Madson, C. & Glenn, R., The Use of HMAC-SHA-1-96 within ESP and AH, November 1998, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2404.txt>>

- [28] Maughan, D. & Schertler, M. & Schneider, M. & Turner, J., Internet Security Association and Key Management Protocol (ISAKMP), November 1998, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2408.txt>>
- [29] Myers, M. & Ankney, R. & Malpani, A. & Galperin, S. & Adams, C., X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP, June 1999, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2560.txt>>
- [30] National Institute of Standards and Technology, Advanced Encryption Standard, 5.3.2001, [referred 27.6.2001]  
<<http://csrc.nist.gov/encryption/aes/>>
- [31] Nystrom, M. & Kalinski, B., PKCS #10: Certification Request Syntax Specification Version 1.7, November 2000, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2986.txt>>
- [32] Orman, H., The Oakley Key Determination Protocol, November 1998, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2412.txt>>
- [33] PGP Security, Gauntlet VPN, [referred 27.6.2001]  
<<http://www.pgpinternational.com/products/vpnsuite/default.shtml>>
- [34] RSA Security, Keon, [referred 27.6.2001]  
<<http://www.rsa.com/products/keon/index.html>>
- [35] RSA Security, SecurID, [referred 27.6.2001]  
<<http://www.rsasecurity.com/products/securid/index.html>>
- [36] Schneier, B., Applied Cryptography Second Edition: protocols, algorithms, and source code in C, John Wiley & Sons, New York, 1996, 758 p.

- [37] Silverman, R. D., A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, April 2000, [referred 27.6.2001]  
<<ftp://ftp.rsasecurity.com/pub/pdfs/bulletn13.pdf>>
- [38] SmartTrust, [referred 27.6.2001]  
<<http://www.smarttrust.com/>>
- [39] Stonesoft, StoneGate, [referred 27.6.2001]  
<<http://www.stonesoft.com/document/143.html>>
- [40] Symantec, Symantec Enterprise Firewall 6.5, [referred 27.6.2001]  
<<http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=47&PID=5718284>>
- [41] Tivoli, IBM SecureWay Directory, [referred 27.6.2001]  
<<http://www.ibm.com/software/network/directory/index.html>>
- [42] Tivoli, IBM SecureWay Firewall, [referred 27.6.2001]  
<[http://www.tivoli.com/products/index/secureway\\_firewall/index.html](http://www.tivoli.com/products/index/secureway_firewall/index.html)>
- [43] Wahl, M. & Howes, T. & Kille, S., Lightweight Directory Access Protocol (v3), December 1997, [referred 27.6.2001]  
<<ftp://ftp.isi.edu/in-notes/rfc2251.txt>>
- [44] Xiaoyi, L. & Madson, C. & McGrew, D. & Nourse, A., Cisco System's Simple Certificate Enrollment Protocol, 1998, [referred 27.6.2001]  
<[http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep\\_wp.pdf](http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.pdf)>

# Appendix A

## Reference System Specifications

### VPN Gateway

- Sun Ultra 10
  - 440 MHz UltraSPARC-IIi, 2 MB level 2 cache
  - 512 MB PC133 DIMM main memory
  - 20 GB IDE hard drive
  - Quad FastEthernet 10/100 Mbps Network Interface Card
- Solaris 2.6
  - Kernel patch 105181-23
  - Quad FastEthernet PCI Adapter driver version 1.38
- CheckPoint FW-1/VPN-1 version 4.1 Service Pack 1 (2000 edition) [3]
  - Key management protocols: Internet Key Exchange, FWZ (CheckPoint proprietary) and SKIP.
  - Encryption algorithms: 3DES, CAST, DES, FWZ-1 (CheckPoint proprietary).
  - Authentication algorithms: SHA-1, MD5.
  - User authentication mechanisms: RADIUS, TATACS/TATACS+, token-based (two factor), operating system password, FireWall-1 password, S/KEY, digital certificates.

## Certificate Authority

- Fujitsu-Siemens Scenic T, i815E
  - 1000 MHz Intel Pentium III, 256 kB level 2 cache
  - 256 MB PC133 SDRAM DIMM
  - 20 GB IDE hard drive
  - Integrated Intel 82562ET network interface controller
- Windows 2000 Service Pack 2
- RSA Keon Sentry CA 4.7 [34]
  - Administration Server listening on port 443
  - Enrollment Server listening on port 444
  - SCEP Server listening on port 446
  - CRL Server listening on port 447
  - Secure Directory (LDAP directory) Server listening on port 389