



Tampereen teknillinen yliopisto  
Tietotekniikan osasto

Teemu Alakoski

## **Avainten vaihto ja jakelu IPSec-järjestelmässä**

Diplomityö

Aihe hyväksytty osastoneuvoston kokouksessa 12.3.2003

Tarkastajat: Prof. Jarmo Harju

FT Jukka Koskinen

# Alkusanat

Tämä diplomityö on tehty osana ICEFIN-projektia Tampereen teknillisen yliopiston tietoliikennetekniikan laitoksella. Työssä käytetty koeverkko rakennettiin tietoliikennetekniikan laitoksen verkkolaboratorioon.

Haluan kiittää professori Jarmo Harjua ja lehtori Jukka Koskista työni ohjaamisesta, Heikki Vatiaista oikeanlaisen tutkimusasetteen opettamisesta, Jussi Lemposta ja Sami Keski-Kasaria avusta käytännön ongelmissa sekä Ilkka Vesaa avusta tietoturvaan liittyvissä kysymyksissä. Lisäksi haluan kiittää isoveljeäni Jani Alakoskea, jonka ansiosta olen tietoliikennetekniikan pariin siirtynyt, sekä kihlattuani Satu Kootaa henkisestä tuesta.

Työ on kirjoitettu Juha Laineen ja Jussi Lemposen tekemää  $\text{\LaTeX}$ -pohjaa käyttäen.

Tampere, 16.4.2003

Teemu Alakoski

Vaajakatu 5 A 17

33720 Tampere

Finland

teemu.alakoski@iki.fi

# Tiivistelmä

## TAMPEREEN TEKNILLINEN YLIOPISTO

Tietotekniikan osasto

Tietoliikennetekniikan laitos

**Teemu Alakoski:** Avainten vaihto ja jakelu IPSec-järjestelmässä

Diplomityö: 65 sivua

Tarkastajat: Prof. Jarmo Harju ja FT Jukka Koskinen

Huhtikuu 2003

Internetin käytön levitessä uusille, luottamuksellisuutta vaativille alueille kuten pankkiasioiden hoitoon, etätyöntekoon ja viranomaisten väliseen henkilötietojen välitykseen, tietoturvan merkitys kasvaa jatkuvasti. Yhtenäisellä tavalla tietoliikenteelle tietoturvaa tarjoavan menetelmän käyttömahdollisuuksia tulee aktiivisesti tutkia, jotta mahdollisimman suuri osa verkkoliikenteestä kulkisi suojattuna ilman erilaisten suojausmenetelmien viidakkoa. Yksi yhtenäinen viitekehys on verkkoliikennettä IP-tasolla suojaava IP Security Protocol (IPSec).

Tässä työssä on tutkittu IPSec-järjestelmän laaja-alaisessa käytössä välttämättömiä osaluueita: julkisten avainten jakelumenetelmiä ja julkisia avaimia autentikointiin käyttäviä avaintenvaihtoprotokollia, jotka liittyvät IPSec-turvallisuusassosiaatioiden dynaamiseen luontiin. Avaintenvaihtoprotokollissa keskitytään IPSec-protokollaperheen tällä hetkellä käyttämään IKE-protokollaan ja sen seuraajaksi suunniteltuihin IKEv2- ja JFK-protokolleihin.

Menetelmien ominaisuuksien käsittelyn lisäksi työssä analysoidaan niiden heikkouksia ja vahvuuksia sekä ehdotetaan kullekin sopivinta käyttöympäristöä. Julkisten autentikointiavainten jakelumenetelmien osalta apuna käytetään kokemuksia, joita on saatu tekemällä käytännön testejä sitä varten rakennetussa testiverkossa.

# Abstract

## TAMPERE UNIVERSITY OF TECHNOLOGY

Department of Information Technology

Institute of Communications Engineering

**Teemu Alakoski:** Key exchange and distribution in IPSec system

Master of Science thesis: 65 pages

Supervisors: Prof. Jarmo Harju and PhD Jukka Koskinen

April 2003

The use of Internet is spreading to new security-conscious areas such as bank transactions, telecommuting and exchange of person register related information between authorities. This progress increases the significance of information security. We should actively explore the possibility to use a mechanism that offers a uniform way to secure telecommunications so that most of Internet communications would be secure without need to use several different tools in parallel. One such uniform context is IP Security Protocol which is used to secure telecommunications at IP-level.

This Master of Science thesis examines a field that is necessary in widespread use of IPSec: distribution methods of public authentication keys and key exchange protocols. A key exchange protocol is a protocol used in dynamic creation of IPSec security associations and often depends on public keys for authentication. This thesis concentrates on the current key exchange protocol used by IPSec and to its two competing successors.

In addition to specifying the characteristics of these methods, this thesis analyzes their weaknesses and strengths, and proposes the most suitable environment for each of them. A test network was built for the purpose, and experiences gained with the network are used to support the analysis of the distribution methods of the public authentication keys.

# Sisällysluettelo

<b>Alkusanat</b> . . . . .	i
<b>Tiivistelmä</b> . . . . .	ii
<b>Abstract</b> . . . . .	iii
<b>Sisällysluettelo</b> . . . . .	iv
<b>Lyhenneluettelo</b> . . . . .	vi
<b>1 Johdanto</b> . . . . .	1
<b>2 IPSec</b> . . . . .	3
2.1 IPSec-moodit . . . . .	4
2.2 IPSec-protokollat . . . . .	5
2.2.1 Authentication Header . . . . .	5
2.2.2 Encapsulating Security Payload . . . . .	6
2.3 Turvallisuusassosiaatiot ja SPI . . . . .	7
2.4 Security Policy Database . . . . .	8
<b>3 Avaimet ja sertifikaatit</b> . . . . .	9
3.1 X.509 -sertifikaatit . . . . .	9
3.2 Diffie-Hellman -avaintenvaihto . . . . .	12
3.3 Ennalta sovittu avain, PSK . . . . .	13
<b>4 Avaintenvaihtoprotokollat</b> . . . . .	15
4.1 IKE . . . . .	16
4.1.1 ISAKMP . . . . .	17
4.1.2 IPSec DOI . . . . .	20
4.1.3 Vaiheet . . . . .	20
4.1.4 Vaihdot . . . . .	21
4.1.5 Autentikointimenetelmät . . . . .	22
4.1.6 Algoritmeista sopiminen . . . . .	25
4.2 IKEv2 . . . . .	26
4.2.1 Muutokset vanhasta versiosta . . . . .	26
4.2.2 Ensimmäinen vaihe . . . . .	27
4.2.3 Toinen vaihe . . . . .	30
4.2.4 Algoritmeista sopiminen . . . . .	32
4.2.5 Yhteensopivuus osoitteenmuunnoksen kanssa . . . . .	32
4.2.6 Ulkoiset autentikointimenetelmät . . . . .	34
4.3 JFK . . . . .	35
4.3.1 Suunnitteluperiaatteet . . . . .	35
4.3.2 Toiminta . . . . .	36
4.3.3 Ominaisuudet . . . . .	37
<b>5 Julkisten avainten jakelu</b> . . . . .	39

5.1	Certificate Payload . . . . .	40
5.2	Opportunistic Encryption . . . . .	42
	5.2.1 Toiminta . . . . .	42
	5.2.2 Kryptografisesti suojattu nimipalvelu, DNSSEC . . . . .	44
5.3	LDAP . . . . .	45
5.4	Muita keinoja . . . . .	46
<b>6</b>	<b>Käytännön testaus . . . . .</b>	<b>47</b>
6.1	Oman sertifiikaatin lähettäminen . . . . .	49
6.2	Nimipalvelu sertifiikaattien jakelumethodina . . . . .	49
6.3	LDAP sertifiikaattien jakelumethodina . . . . .	51
<b>7</b>	<b>Eri menetelmien analyysi . . . . .</b>	<b>54</b>
7.1	Avaintenvaihtoprotokollat . . . . .	54
	7.1.1 Montako vaihetta . . . . .	55
	7.1.2 Algoritmien neuvottelu . . . . .	57
	7.1.3 Monimutkaisuus . . . . .	58
7.2	Avainten jakelumenetelmät . . . . .	59
	7.2.1 Yleiset ominaisuudet . . . . .	59
	7.2.2 Suorituskyky ja saatavuus . . . . .	60
	7.2.3 Skaalautuvuus . . . . .	61
	7.2.4 Oikea ympäristö . . . . .	62
<b>8</b>	<b>Yhteenveto . . . . .</b>	<b>64</b>
	<b>Lähdeluettelo . . . . .</b>	<b>66</b>

# Lyhenneluettelo

<b>AH</b>	Authentication Header
<b>ASN.1</b>	Abstract Syntax Notation number One
<b>BER</b>	Basic Encoding Rules
<b>CA</b>	Certification Authority
<b>CBC</b>	Cipher Block Chaining
<b>CIP</b>	Common Indexing Protocol
<b>CRL</b>	Certificate Revocation List
<b>DAP</b>	Directory Access Protocol
<b>DNS</b>	Domain Name System
<b>DNSSEC</b>	Domain Name System Security Extensions
<b>DoS</b>	Denial of Service
<b>DSP</b>	Directory Service Protocol
<b>EAP</b>	Extended Authentication Protocol
<b>ESP</b>	Encapsulating Security Payload
<b>FTP</b>	File Transfer Protocol
<b>HMAC</b>	Keyed-Hash Message Authentication Code
<b>HTTP</b>	Hypertext Transfer Protocol
<b>IETF</b>	Internet Engineering Task Force
<b>IKE</b>	Internet Key Exchange
<b>IP</b>	Internet Protocol
<b>IPSec</b>	Internet Protocol Security
<b>ISAKMP</b>	Internet Security Association and Key Management Protocol
<b>ISO</b>	International Organization for Standardization

<b>JFK</b>	Just Fast Keying
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>MAC</b>	Message Authentication Code
<b>NAPT</b>	Network Address and Port Translation
<b>NAT</b>	Network Address Translation
<b>OE</b>	Opportunistic Encryption
<b>OSI</b>	Open System Interconnection
<b>OSPF</b>	Open Shortest Path First
<b>PCP</b>	Payload Compression Protocol
<b>PFS</b>	Perfect Forward Secrecy
<b>PKI</b>	Public Key Infrastructure
<b>PSK</b>	Preshared Key
<b>SA</b>	Security Association
<b>SADB</b>	Security Association Database
<b>SPD</b>	Security Policy Database
<b>SPI</b>	Security Parameter Index
<b>SSL</b>	Secure Sockets Layer
<b>TCP</b>	Transmission Control Protocol
<b>TLS</b>	Transport Layer Security
<b>URL</b>	Uniform Resource Locator
<b>VPN</b>	Virtual Private Network
<b>WAN</b>	Wide Area Network

# 1 Johdanto

Internet Protocol Security (IPSec) on protokollaperhe, jonka avulla on mahdollista salata osapuolten välinen TCP/IP -liikenne. IPSec määrittelee hyvin kattavasti analysoidut protokollat luottamuksellisuuden ja eheyden varmistamiseksi. Jotta näistä ominaisuuksista saataisiin konkreettista hyötyä, on tiedonsiirron toinen osapuoli ensin tunnistettava luotettavasti ja siten, että menetelmä skaalautuu myös laajempaan käyttöön. Tätä varten IPSec-protokollaperhe sisältää IKE-avaintenvaihtoprotokollan (Internet Key Exchange), jonka tehtävänä on dynaamisesti luoda tietoturva-assosiaatioita sekä neuvotella salausavaimet tietoturvaprotokollien käyttöön.

Viime vuosina on kuitenkin käynyt ilmi, että erittäin modulaariseksi ja monikäyttöiseksi suunniteltu IKE on liian monimutkainen implementoida, ja lisäksi siitä on löydetty useita haavoittuvuuksia. IETF (Internet Engineering Task Force) on tilanteen korjaamiseksi aloittanut uuden version määrittelyn ja tuloksena on kaksi erilaista ehdotusta IKE:n seuraajaksi, JFK (Just Fast Keying) ja IKEv2. Määrittelytyön aikana on ilmennyt poikkeavia mielipiteitä menetelmistä, joilla avaintenvaihtoa suorittavat osapuolet saavat haltuunsa autentikoinnissa tarvittavat julkisen avaimen kryptografiaan perustuvat sertifikaatit. Vaihtoehtoisia menetelmiä on muutamia ja niiden heikkoudet ja vahvuudet on tärkeää analysoida ennen järjestelmän käyttöönottoa.

Tässä diplomityössä kerrotaan avaintenvaihtoprotokollien – nykyisen version ja uusien ehdokkaiden – toimintaperiaatteet, ominaisuudet ja suunnittelussa painotetut näkökohdat, tuodaan esille heikkoudet ja vahvuudet sekä annetaan kritiikkiä. Työssä esitellään myös vaih-

toehdot julkisten avainten jakelulle sekä testataan kolme yleisimmin käytössä olevaa vaihtoehtoa, certificate payload, LDAP ja opportunistic encryption, tätä tarkoitusta varten rakennetussa testiverkossa. Testiverkon käyttökokemusten perusteella analysoidaan eri menetelmien ominaisuuksia sekä niiden heikkouksia ja vahvuuksia. Lisäksi kerrotaan millaiseen ympäristöön kukin järjestelmä sopii parhaiten. Varsinaista avaintenvaihtoprotokollien suorittamaa salausavainten luomista ei käsitellä, koska se on varsin mekaaninen toimenpide ja helposti luettavissa protokollan määrittelystä.

Luku 2 on johdanto IPSec-määrittelyyn. Se esittelee protokollaperheen toiminnan, erilaiset toimintamoodit ja tietoturvaprotokollat. Luvussa esitellään suojauksen aiheuttamat muutokset pakettiformaattiin sekä jatkon kannalta tärkeimmät käsitteet.

Liikenteen salaukseen tarvittavien salausavainten ja sertifikaattien sekä salausavainten luomisen perusteet kerrotaan luvussa 3. Luvussa 4 käsitellään avaintenvaihtoprotokollat ja luvussa 5 avaintenjakelumenetelmät, joiden testaus on kerrottu luvussa 6.

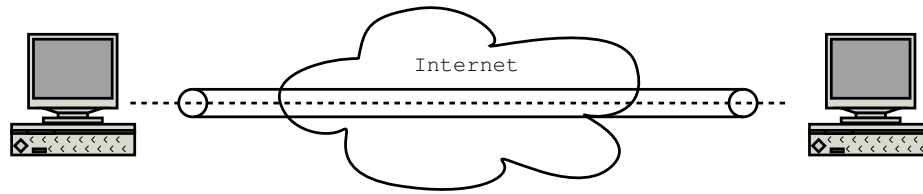
Luvussa 7 tehdään analyysi diplomityössä tarkastelluista menetelmistä ja yhteenveto koostaan luvussa 8.

## 2 IPSec

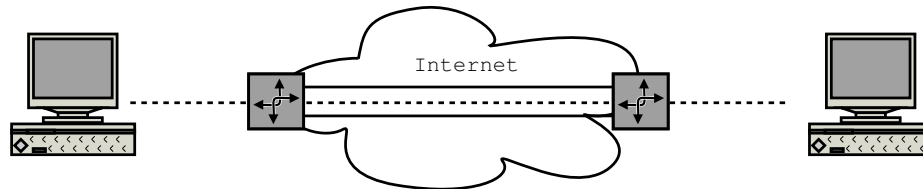
Internet Protocol Security (IPSec) on Internet Engineering Task Forcen (IETF) määrittelemä sarja protokollia, jotka yhdessä muodostavat tietoturvapalveluita tarjoavan kokonaisuuden. Nämä palvelut ovat: pääsynvalvonta, yhteydetön eheys, autentikointi, luottamuksellisuus, suoja uudelleenlähetyksiä vastaan sekä osittainen suoja liikenneanalyysiä vastaan [1, s. 4]. Palvelu toimii verkkokerroksella tarjoten suojan myös kaikille ylemmille protokollakerroksille.

IPSec määrittelee tavan kertoa, mikä liikenne suojataan, miten suojataan ja mihin liikenne lähetetään. Liikennettä voidaan suojata kahden työaseman, kahden reitittimen tai työaseman ja reitittimen välillä. Koska suojattu IP-paketti on myös IP-paketti, on tietoturvapalveluiden kerrostaminen mahdollista käyttämällä tietoturvapalvelua jo suojattuun IP-pakettiin. [2, s. 42]

IPSec -arkkitehtuuri määrittelee tietoturvaprotokollat, avaintenvaihtoprotokollan sekä pakolliset kryptografiset algoritmit. Tietoturvaprotokollia on kaksi, Authentication Header (AH) ja Encapsulating Security Payload (ESP). Avaintenvaihtoprotokolla on Internet Key Exchange (IKE) [3].



Kuva 2.1: Kuljetus-moodi kahden työaseman välillä [2, s. 64]



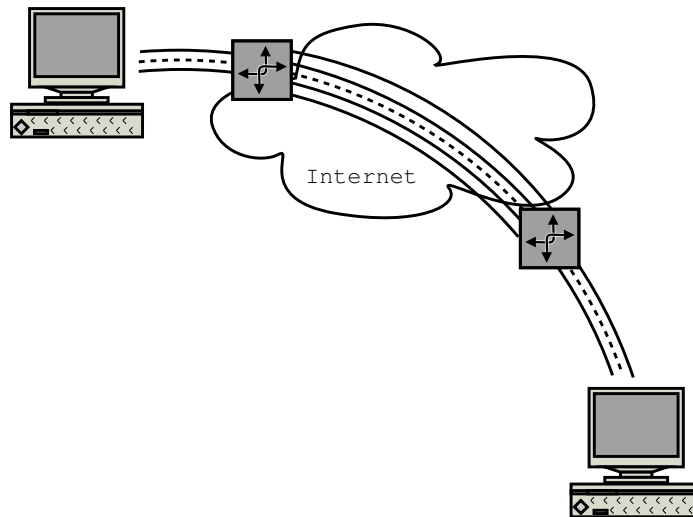
Kuva 2.2: Tunneli-moodi kahden reitittimen välillä [2, s. 66]

## 2.1 IPSec-moodit

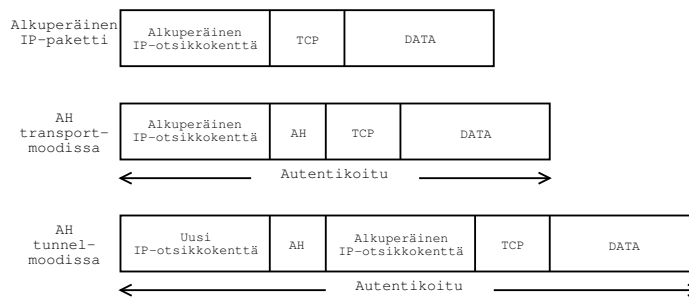
Liikennettä voidaan suojata joko tunneli- tai kuljetus-moodissa. Moodi ei vaikuta algoritmeihin eikä protokoliin sinänsä, kyse on siitä mitä suojataan. Tunneli-moodissa suojataan koko IP-datagrammi ja kuljetus-moodissa hyötydata sekä osa otsikkokentistä.

Kuljetus-moodia käytetään, kun liikenne halutaan suojata kahden työaseman välillä, kuten kuvassa 2.1. Tällöin otsikkokentän ja hyötydatan väliin lisätään uusi otsikkokenttä, joka käytettävästä tietoturvaprotokollasta riippuen sisältää autentikointiin tai autentikointiin ja salaukseen liittyvää informaatiota. Paketin hyötydata sekä osa otsikkokentistä suojataan paketin muuten pysyessä ennallaan.

Tunneli-moodin avulla voidaan suojata reittimien takana olevien aliverkkojen välinen liikenne. Tällöin reititin luo uuden IP-paketin jonka hyötykuormaksi tulee suojattava datagrammi. Menetelmä vastaa kuljetus-moodia tilanteessa, jossa hyötydatana on koko alkuperäinen IP-paketti. Tunnelin toisessa päässä reititin purkaa paketin ja lähettää hyötykuormana olleen IP-paketin oikealle työasemalle. Tällöin uloimman otsikkokentän kohdeosoitteena on aina tunnelin päässä olevan reitittimen osoite riippumatta lopullisesta vastaanottajakoneesta. Tämä lisää turvallisuutta vaikeuttamalla esimerkiksi liikenneanalyysiä. Tällainen menettely on esitetty kuvassa 2.2. Tunneli voi alkaa tai loppua myös työasemaan ja tunneliteita voi myös kerrostaa kuten kuvassa 2.3.



Kuva 2.3: Sisäkkäiset tunnelit



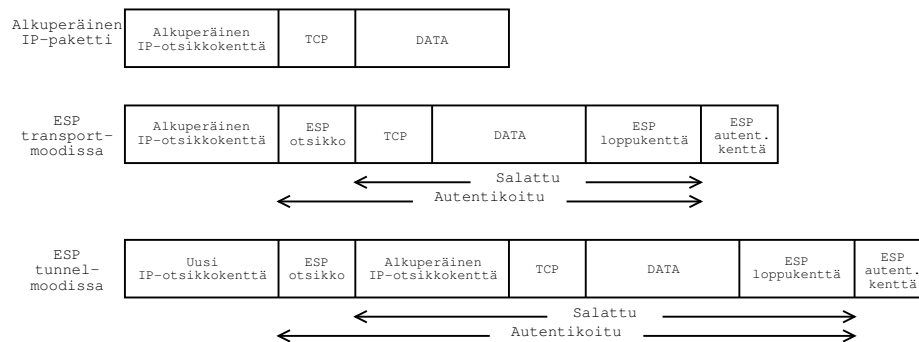
Kuva 2.4: AH kuljetus- ja tunneli-moodissa

## 2.2 IPSec-protokollat

### 2.2.1 Authentication Header

AH tarjoaa eheyden, autentikoinnin ja suojan uudelleenlähetyksiä vastaan liittämällä pakettiin protokollakenttien paketin sarjanumeron ja avaimen yli lasketun tiivisteen. Tiivisteseen otetaan mukaan kaikki kentät, joiden arvo määräytyy jo pakettia lähetettäessä. Kentät, joiden arvoa ei voi ennalta tietää, nollataan tiivistettä laskettaessa. Tällaisia kenttiä ovat muun muassa reitityssolmuja laskevat kentät sekä palvelunlaatuun liittyvät kentät. Tunneli-moodissa AH siis suojaa sekä ulomman että sisemmän IP-paketin otsikkokenttiä.

AH lisää pakettiin uuden otsikkokentän, joka sijaitsee IP-otsikkokentän ja suojattavan datan välissä. Kuvassa 2.4 on esitetty otsikkokenttien sijoittuminen IP-datagrammiin.



Kuva 2.5: ESP kuljetus- ja tunneli-moodissa

Tiivisteen laskemiseen käytettäviä – kaikissa implementaatioissa mukana olevia – algoritmeja ovat HMAC-MD5-96 [4] ja HMAC-SHA-1-96 [5]. Määritelmä sallii myös muiden algoritmien käytön ja tietokoneiden laskentatehon koko ajan kasvaessa uusia algoritmeja tulevaisuudessa todennäköisesti otetaankin käyttöön.

## 2.2.2 Encapsulating Security Payload

ESP tarjoaa AH:n tarjoamien palveluiden lisäksi luottamuksellisuuden. Eheys, autentikointi ja suoja uudelleenlähetyksiä vastaan toteutetaan – kuten AH:ssakin – tiivistefunktioiden avulla. Luottamuksellisuus saavutetaan käyttämällä salausalgoritmeja. Uuden otsikkokentän lisäksi ESP vaatii datagrammiin loppukentän. ESP suojaa vain otsikko- ja loppukenttensä välisen osan IP-paketista, joten IP-otsikkokentistä vain sisempi on suojattu tunneli-moodia käytettäessä. Kuvassa 2.5 on esitetty otsikkokenttien sijainti.

Käytettävät tiivistefunktiot ovat samat kuin AH:ssakin. RFC2406 [6] määrittelee pakollisiksi salausalgoritmeiksi DES-CBC [7] ja NULL [8]. DES-CBC:tä ei yleisesti pidetä enää turvallisena algoritmina ja toteutuksissa onkin kehoitettu käyttämään ESP\_3DES:iä sen tilalla [9]. Uudeksi salausalgoritmiksi todennäköisesti tulee AES [10] Cipher Block Chaining -moodissa (CBC) [11] tai Counter -moodissa (CTR) [12].

## 2.3 Turvallisuusassosiaatiot ja SPI

Turvallisuusassosiaatio (Security Association, SA) on abstraktio kahden verkkolaitteen välisen liikenteen suojauksen parametreille. Se on perusta kaikelle suojatulle liikenteelle IPSec-järjestelmässä. IPSec SA määrittelee käytettävän protokollan, algoritmit, avaimen ja avaimen eliniän.

IPSec SA on yksisuuntainen; kahden tietokoneen väliseen keskusteluun tarvitaan vähintään kaksi turvallisuusassosiaatiota. Lisäksi yksi IPSec SA määrittelee vain yhden käytettävän tietoturva-protokollan, joten jos halutaan käyttää useampaa protokollaa yhtäaikaan, on turvallisuusassosiaatioita luotava useampia.

Jokainen IPSec-järjestelmää käyttävä kone pitää yllä turvallisuusassosiaatioiden tietokantaa (Security Association Database, SADB), jossa turvallisuusassosiaatio yksilöidään SPI:n (Security Parameter Index), IP-kohdeosoitteen ja IPSec-protokollan perusteella. Näiden tietojen perusteella voidaan vastaanotettuun liikenteeseen soveltaa oikeita algoritmeja. Turvallisuusassosiaatioiden yksisuuntaisuudesta johtuen lähtevälle ja saapuvalla liikenteelle on omat taulunsa turvallisuusassosiaatitietokannassa.

Käsin yksitellen määriteltävät turvallisuusassosiaatiot eivät skaalaudu hyvin laajempaan käyttöön, koska käytettävät parametrit on sovittava turvallista siirtotietä, esimerkiksi puhelinta, käyttäen. Tämä on työlästä ja virheiden mahdollisuus on suuri parametreja käsin syötettäessä. IETF on määritellyt avaintenvaihtoprotokollan IKE, joka osaa luoda IPSec SA:t dynaamisesti silloin kun uusi suojattu yhteys halutaan muodostaa. Tätä varten avaintenvaihtoon osallistuvat prosessit luovat oman kaksisuuntaisen turvallisuusassosiaationsa (IKE SA), jonka suojassa sovitaan IPSec SA:n protokolla, algoritmit, parametrit ja avain.

SPI on 32-bittinen luku, joka on mukana jokaisessa IPSec:illä suojatussa paketissa. SPI:tä käytetään, koska vastaanottajalla on oltava jokin keino erotella eri turvallisuusassosiaatioihin kuuluvat paketit, joissa vastaanottajan osoite ja IPSec-protokolla ovat samat.

Vastaanottaja päättää SPI:n uutta turvallisuusassosiaatiota luodessaan ja kertoo tämän toiselle osapuolelle. Vastaanottaja valitsee SPI:n siten, että kolme arvoa, SPI, IP-kohdeosoite ja IPSec-protokolla yksilöivät IPSec SA:n. Kun turvallisuusassosiaatio vanhenee tai se tuhoetaan, voi SPI:n käyttää uudelleen.

## 2.4 Security Policy Database

RFC2401:n määrittelemässä IPSec-toteutuksen mallissa on kaksi tietokantaa, Security Policy Database (SPD) ja Security Association Database (SADB). Ensimmäinen kuvaa tietoturvapoliitiikan, jota sovelletaan sisääntulevaan ja ulosmenevään liikenteeseen. Jälkimmäinen sisältää jokaiseen turvallisuusassosiaatioon liittyvät parametrit. Vaikka RFC2401 ei määrää tietorakenteiden muotoa ja rajapintaa, on tietyt toiminnalliset ominaisuudet sovittu, jotta eri implementaatioiden yhteensopivuus olisi todennäköisempää. [1]

SPD:n pitää erotella IPSec-suojauksen vaativa liikenne sekä liikenne jota ei suojata. Jokaiselle tulevalle tai lähtevälle paketille on kolme eri toimintamallia: hylätään, ohitetaan IPSec tai käsitellään IPSec:in avulla. Ensimmäinen vaihtoehto tarkoittaa tilannetta, jossa kyseisen liikenteen ei sallita lähtevän tai saapuvan ollenkaan. Toinen toimintamalli on liikenteelle, joka ei tarvitse suojausta. Kolmas tilanne on liikenteelle, joka halutaan suojata. Tällöin SPD määrittelee käytettävät tietoturvapalvelut, protokollat ja algoritmit. [1]

Tietokanta sisältää listan liikenteelle sovellettavia tietoturvapoliitikoita. Liikenne erotellaan valitsimiksi kutsuttujen kenttien perusteella. Valitsimia ovat muunmuassa lähde- ja kohdeosoitteet, kuljetuskerroksen protokolla ja TCP- tai UDP-portit. Näiden kenttien perusteella liikennettä prosessoitaessa voidaan tehdä päätös liikenteen suojaamisesta, suojaamatta jättämisestä tai estämisestä. Poliitiikan vaatiessa liikenteen suojaamista, on SPD:stä osoitin SADB:hen, joka kertoo, mikä SA on kyseistä liikennettä varten. Osoittimen puuttuminen kertoo, että SA:ta ei ole luotu. Tällöin pitää käynnistää avaintenvaihtoprotokolla turvallisuusassosiaation luomiseksi.

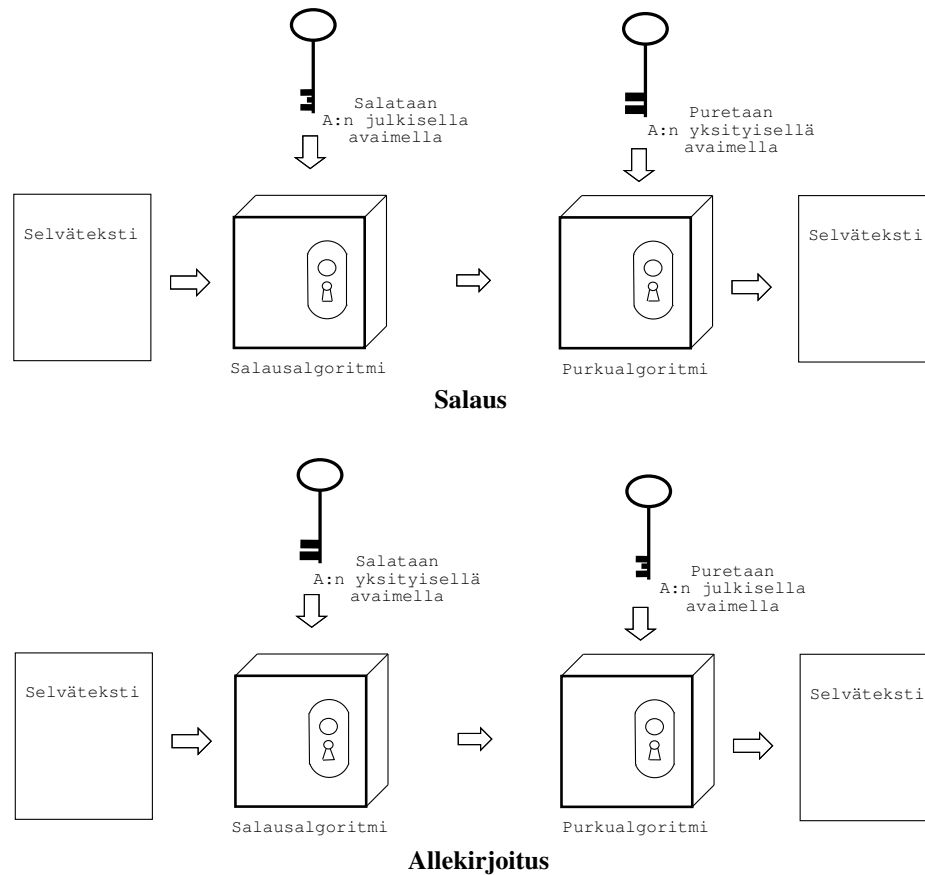
## 3 Avaimet ja sertifikaatit

Salausavain ja salattava teksti yhdessä muodostavat salausalgoritmin syötteen. Riippuen algoritmista, avaimelta vaaditaan erilaisia ominaisuuksia. Julkisen avaimen menetelmä perustuu kahden matemaattisesti toisiinsa liittyvän avaimen käyttöön: toista (julkista) avainta käytetään viestin salaamiseen, jonka vain sitä vastaavalla toisella (yksityisellä) avaimella voi avata. Julkisen avaimen menetelmän etuna on, että haluttaessa lähettää jollekin salattu viesti, voidaan käyttää tämän yleisesti esillä olevaa julkista avainta. Viestin saaja purkaa salauksen käyttämällä yksityistä avaintaan. Menetelmä on paljon joustavampi kuin perinteisen kryptografian mahdollistamat keinot, joissa tarvitaan osapuolten välinen sopimus yhteisestä salausavaimesta. Julkisen avaimen menetelmää voidaan soveltaa sekä salauksessa että allekirjoituksessa (kuva 3.1).

Nykyaikaiseen – skaalautuvaan – kryptografian tarpeeseen on kehitetty sertifikaatit, jotka kolmannen osapuolen varmistamina sitovat yhteen identiteetin ja sitä vastaavan julkisen avaimen. Tässä luvussa kuvataan yleisimmän käytössä olevan julkisen avaimen sertifikaatin rakenne sekä mekanismi salausavainten vaihtamiseksi. Lisäksi kuvataan symmetrisen salauksen käyttämän salausavaimen ominaisuuksia.

### 3.1 X.509 -sertifikaatit

Varmenne eli sertifikaatti on kolmannen osapuolen varmentama sähköinen dokumentti, joka sisältää varmenteen kohteena olevan osapuolen identiteetin ja julkisen avaimen sekä var-

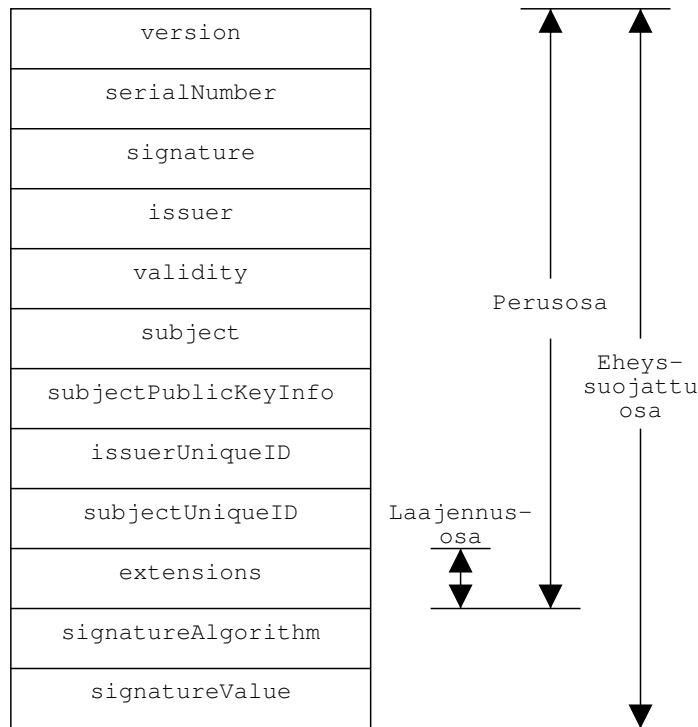


Kuva 3.1: Salaus ja autentikointi julkisen avaimen menetelmällä [13, s. 671]

mentajan laskeman digitaalisen allekirjoituksen. Jos sertifikaatin sisältöä muutetaan, ei se enää vastaa digitaalista allekirjoitusta. Digitaalisen allekirjoituksen voi tehdä vain luotettu kolmas osapuoli omalla yksityisellä avaimellaan. Sertifikaatin sisältöä ei siis voi muuttaa siten että sitä ei huomattaisi. Tämä helpottaa huomattavasti sertifikaattien jakelua, koska sertifikaattien jakelupisteiden ei tarvitse nauttia PKI:n (Public Key Infrastructure) osapuolten luottamusta, eikä jakelumenetelmän tarvitse olla kryptografisesti suojattu.

X.509 -sertifikaatti on yleisimmin käytetty julkisen avaimen sertifikaatti. Se on alunperin tarkoitettu X.500 -standardin mukaisen hakemiston autentikointia varten. Käyttötarkoitus on kuitenkin muuttunut alkuperäisestä, ja X.509 -sertifikaatti mielletään nykyään yleisesti PKI:n sertifikaattimuodoksi. Tätä tarkoitusta varten sertifikaattiin on määritelty useita laajennuksia. IETF on RFC3280:ssa [14] määritellyt X.509 -sertifikaattien käytön Internetissä.

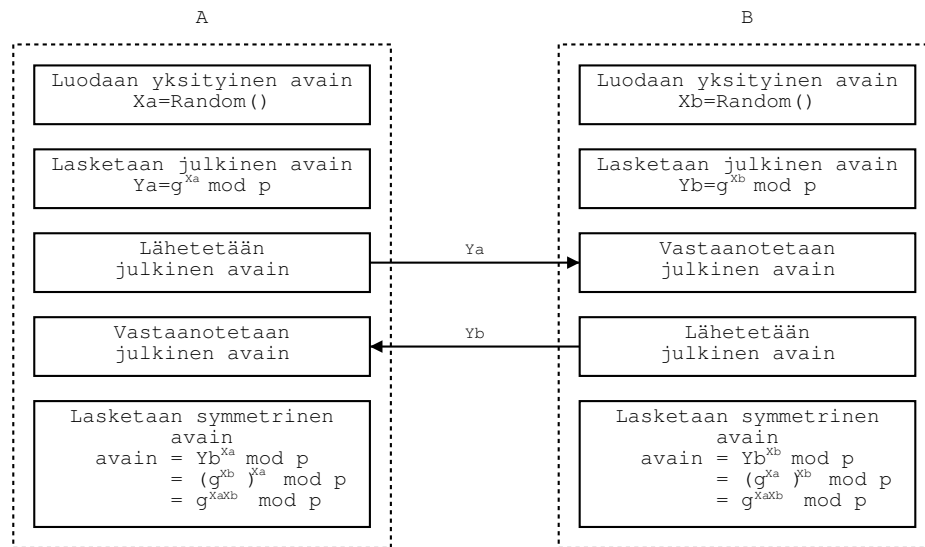
X.509 -sertifikaatti koostuu kolmesta loogisesta osasta: eheysuojatusta osasta, sertifikaatin perusosasta sekä laajennusosasta (kuva 3.2). Uloin, eheysuojattu, osa sisältää kolme kent-



Kuva 3.2: X.509 -sertifikaatin rakenne [15, s. 75]

tää: allekirjoitettavan sertifikaatin, allekirjoituksessa käytettävän algoritmin tunnisteiden ja kolmannen osapuolen tuottaman sertifikaatin autenttisuuden varmistavan digitaalisen allekirjoituksen. Perusosa sisältää sertifikaatin kohteen ja sertifikaatin myöntäjän identifioivat tiedot sekä kohteen hallussa olevaa salaista avainta vastaavan julkisen avaimen. Laajennusosa, joka on jälkikäteen lisätty perusosan sisältöön, sisältää PKI:n kehityksen aikana tarpeellisiksi huomattuja lisäkenttiä, kuten avaimen käyttötarkoitus tai sertifikaattien jake-lupisteen määrittely.

Certificate revocation list (CRL) on samankaltainen dokumentti kuin sertifikaatti. Myös se sisältää tiedot varmentajasta ja tämän laskeman digitaalisen allekirjoituksen. CRL ei kuitenkaan varmenna julkista avainta, vaan listan peruutettujen sertifikaattien sarjanumeroita. Koska jokainen sertifikaatti sisältää sarjanumeron, CRL:n avulla voidaan varmistua, että ei käytetä sertifikaattia, joka on jostain syystä peruutettu. Peruuttamisen syy voi olla esimerkiksi julkista avainta vastaavan salaisen avaimen paljastuminen tai työntekijän poistuminen työnantajansa palveluksesta. CRL on tärkeä osa täysimittaista PKI-järjestelmää.



Kuva 3.3: Diffie-Hellman -avaintenvaihto [15, s. 11]

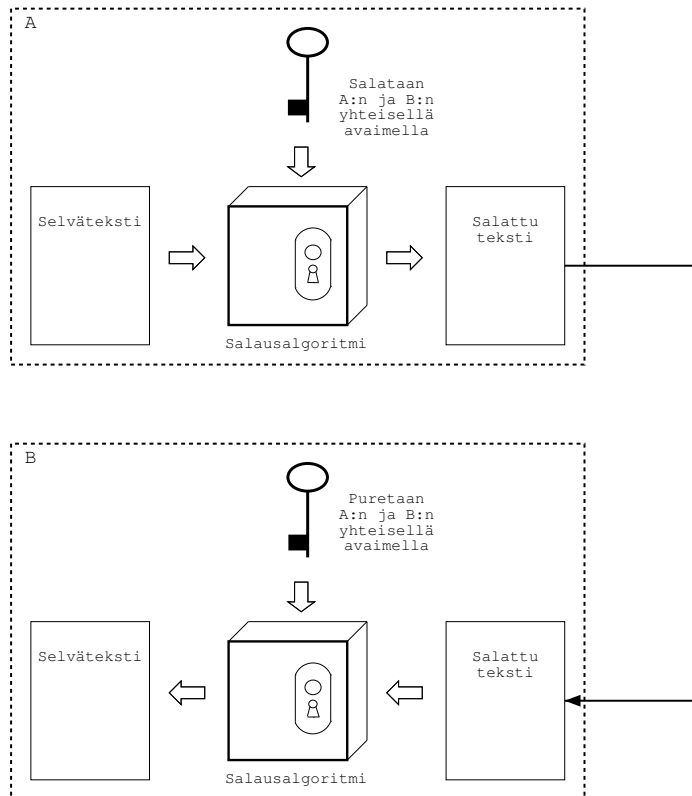
## 3.2 Diffie-Hellman -avaintenvaihto

IPSec -järjestelmän avaintenhallintaprotokolla käyttää salausavainten luomiseen ja vaihtamiseen Whitfield Diffien ja Martin E. Hellmanin kehittämää menetelmää, joka tunnetaan Diffie-Hellman -avaintenvaihtona. IETF:n määrittelemä tapa käyttää Diffie-Hellman -menetelmää on kuvattu RFC2631:ssä [16].

Diffie-Hellman -avaintenvaihto on menetelmä, jonka avulla kaksi osapuolta voivat sopia jaetun salaisuuden siten, että sitä ei voi saada selville salakuuntelemalla yhteyttä. Jaettua salaisuutta voidaan käyttää muodostamaan salausavain osapuolten välisen symmetrisen salausalgoritmin käyttöön.

Osapuolten pitää ensin luoda itsellensä yksityinen avain, sekä tästä johdettu julkinen avain. Tämän jälkeen kumpikin lähettää julkisen avaimensa toiselle osapuolelle. Jaettu salaisuus saadaan lasketuksi oman salaisen ja toisen osapuolen julkisen avaimen avulla. Menetelmä on esitetty kuvassa 3.3.

Menetelmällä luodun avaimen turvallisuuteen vaikuttaa ratkaisevasti julkisen avaimen luomisessa käytetty moduli  $p$  sekä kantaluku  $g$ . Tämän takia IETF on määritellyt näille valmiit, turvallisena pidetyt arvot, joista muodostuvat niin sanotut Diffie-Hellman -ryhmät.



Kuva 3.4: Symmetrinen salaus etukäteen sovittua avainta käyttäen [13, s. 6]

### 3.3 Ennalta sovittu avain, PSK

Ennalta sovittu avain (Preshared Key, PSK) tarkoittaa osapuolten etukäteen valitsemaa yhteistä salausavainta. Tällä menetelmällä salaus ja autentikointi saadaan yleensä kohtuullisen yksinkertaiseksi ja suoraviivaiseksi. Symmetrinen salaus etukäteen sovittulla avaimella on esitetty kuvassa 3.4.

Menetelmän suurin ongelma on skaalautuvuudessa. Jos suojattu tietoliikenneyhteys halutaan muodostaa vain yhden osapuolen kanssa, ei avaimen sopiminen esimerkiksi puhelimitse ole vielä ylivoimaisen hankalaa. Jos osapuolia, joiden kanssa halutaan kommunikoida, on satoja tai tuhansia, on avainten sopiminen kaikkien osapuolten kanssa ylläpidollisesti mahdoton tehtävä. Yleinen symmetrisen salausavaimen pituus voi olla esimerkiksi 128 bittiä. Näin pitkän salausavaimen sopiminen ja syöttäminen manuaalisesti on myös erittäin virheherkkää. Lisäksi avaimen turvallisuuteen vaikuttaa suurelta osin sen satunnaisuus. Ihmisen valitsema avain on usein satunnaisuudeltaan huono. Etukäteen sovittu avaimen luomiseen olisikin käytettävä jotain hyviä satunnaislukuja tuottavaa menetelmää.

PSK on puutteistaan huolimatta usein tietoturvaprotokollissa mukana yhtenä autentikointivaihtoehtona suoraviivaisuutensa vuoksi. Se on hyvä apuväline ryhdyttäessä rakentamaan tietoturvajärjestelmiä sekä yksinkertaistettaessa tilannetta, kun järjestelmässä oleva vika pitää paikallistaa.

## 4 Avaintenvaihtoprotokollat

Olennainen osa turvallisuusassosiaation luomista on salaus- ja autentikointiavaimista sopiminen. Yleisesti tätä kutsutaan avainten vaihdoksi. Avainten vaihto on edellytys suojatun yhteyden luomiselle kahden osapuolen välille.

Avainten vaihto voidaan suorittaa manuaalisesti (PSK), esimerkiksi postin, puhelimen tai muun luotettavaksi katsotun siirtotien avulla. Käytännöllisempi ja nopeampi tapa on kuitenkin dynaaminen avaintenvaihto käyttäen avaintenvaihtoprotokollaa.

Kaksi avaintenvaihtoprotokollaa suorittavaa prosessia pystyvät sopimaan salaus- ja autentikointiavaimet siten, että liikennettä kuuntelevat osapuolet eivät saa niitä tietoonsa. Ongelmaksi muodostuukin vastapuolen luotettava tunnistaminen, koska kahden osapuolen välillä kulkevan liikenteen salaus on turhaa, jos vastapuolta ei voida autentikoida. Etukäteen jaettuja avaimia voidaan käyttää vastapuolen tunnistamiseen myös avaintenvaihtoprotokollaa käytettäessä, mutta tällöin menetetään turvallisuusassosiaatioiden luomisen dynaamisuus. Omimmillaan avaintenvaihtoprotokollat ovatkin julkisen avaimen kryptografiaa hyödyntäviä sertifikaatteja käytettäessä. Sertifikaattien täysimittainen hyödyntäminen vaatii kattavan julkisen avaimen infrastruktuurin (Public Key Infrastructure, PKI). Tätä varten IETF on perustanut pkix-työryhmän kehittämään X.509-sertifikaatteihin perustuvaa PKI:tä.

Tällä hetkellä IPSec-järjestelmän avaintenvaihtoprotokollana käytettävä IKE on implementoijien mielestä liian monimutkainen johtuen sen erittäin monipuolisista neuvotteluominaisuuksista ja modulaarisesta suunnittelusta. Tätä tukee myös se seikka, että vaikka IKE on määritelty jo useita vuosia sitten, eivät eri toteutukset toimi keskenään kovin hyvin. IETF:n

ipsec-työryhmä onkin ruvennut kehittämään IKE:n seuraajaa (Son Of IKE, SOI). Tämä luku kuvaa kahden draftin asteella olevan ehdotuksen, IKEv2:n ja JFK:n (Just Fast Keying), sekä alkuperäisen IKE:n toiminnan.

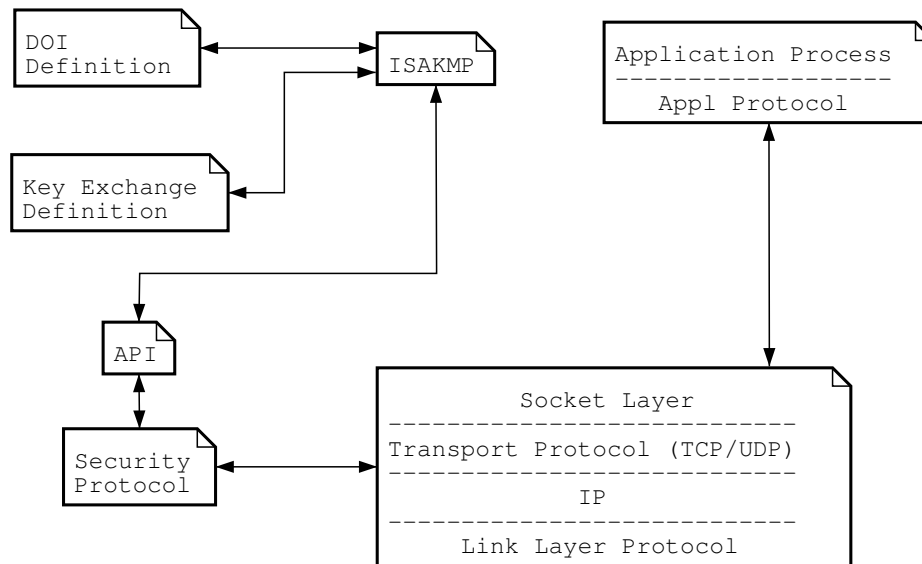
## 4.1 IKE

The Internet Key Exchange on IETF:n määrittelemä avaintenvaihtoprotokolla, jonka tehtävänä on luoda turvallisuusassosiaatioita dynaamisesti. IKE on alunperin tehty IPSec-järjestelmiä varten, mutta geneerisyytensä ansiosta sitä voidaan käyttää luomaan turvallisuusassosiaatioita myös muille protokollille.

IKE on hybridiprotokolla, joka on rakennettu ISAKMP:n [17] määrittelemien raamien sisälle. Se toteuttaa osia kahdesta avaintenhallintaprotokollasta, Oakleystä [18] ja SKEME:stä [19]. Oakleystä on lainattu menetelmä, jossa on eri moodeja autentikoiduille avaintenvaihdoille. SKEME:stä on otettu vaikutteita menetelmässä, jossa osapuolet käyttävät julkisen avaimen salausta vaihtaakseen satunnaisluvut, joista johdetaan osapuolten välinen yhteinen salausavain. [1]

Koko IPSec'in käyttämän avaintenvaihtoprotokollan määrittelee kolme RFC:tä: RFC2407 The Internet IP Security Domain of Interpretation for ISAKMP (DOI) [9], RFC2408 Internet Security Association and Key Management Protocol (ISAKMP) [17] ja RFC2409 The Internet Key Exchange (IKE) [3]. ISAKMP määrittelee yleisen kehyksen ja paketti-formaatit, IKE avaintenvaihtomenetelmät ja DOI kertoo, kuinka edellisiä käytetään neuvoteltaessa turvallisuusassosiaatioita IPSec'in käyttöön. Jokainen protokolla, joka tarvitsee avaintenvaihtoprotokollaa voi määrittellä oman Domain of Interpretation -dokumenttinsa. Kuvassa 4.1 näkyy kuinka eri elementit liittyvät toisiinsa RFC2408:n mukaan.

Ryhdyttyessä luomaan uutta IPSec-turvallisuusassosiaatiota, pitää IKE:n ensin muodostaa oma turvallisuusassosiaationsa, jonka suojassa varsinaiset IPSec SA:t luodaan. IKE SA tarjoaa autentikoidun ja salatun siirtotien. Kuten IPSec SA:ta luotaessa, myös IKE SA:ta luotaessa pitää osapuolten sopia yhteisistä parametreista. Pakolliset neuvoteltavat parametrin ovat: salausalgoritmi, tiivistefunktioalgoritmi, autentikointitapa sekä avainten muodostamiseen liittyvä Diffie-Hellman -ryhmä. Lisäksi voidaan sopia muun muassa IKE SA:n eliniän



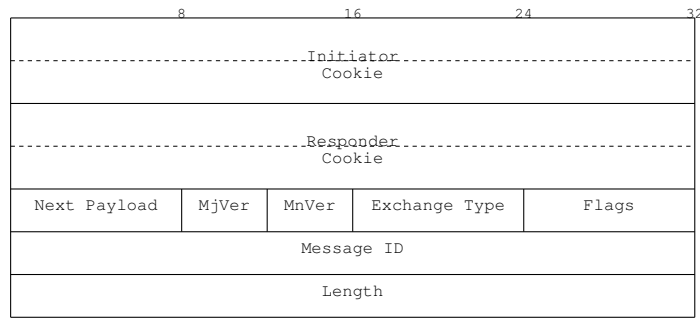
Kuva 4.1: IKE:n, ISAKMP:n ja DOI:n suhde toisiinsa

määräytymisperusteet ja avaimen pituus, jos oletusarvot eivät ole sopivat.

#### 4.1.1 ISAKMP

ISAKMP määrittelee avaintenvaihtoprotokollan pohjan, eli kuinka avaintenvaihdon osapuolet keskustelevat, kuinka vaihdettavat viestit rakentuvat ja tilasiirtymät, joiden kautta suojattu yhteys muodostuu. Se myös määrittelee keinot autentikoida vastapuoli, keinot vaihtaa avaintenvaihtoon liittyvää tietoa sekä keinot neuvotella sovellettavista tietoturvapalveluista. [2]

Koska avaintenvaihtotekniikat ja salaus- ja autentikointialgoritmit on määritelty erillisissä dokumenteissaan, ei ISAKMP ole riippuvainen mistään tietyistä algoritmeista ja avaintenvaihtotekniikoista. Tämä on ollut tietoinen valinta ISAKMP:n suunnitteluvaiheessa ja taustalla on ollut ajatus, että yhteinen turvallisuusassosiaatioiden hallintaan tarkoitettu järjestelmä olisi erittäin geneerinen, kun taas tarkemmat menetelmät on määritelty toisaalla. Tämä parantaa laajennettavuutta ja uusien tehokkaampien menetelmien käyttöönottoa jatkossa. Jos käytössä olevasta menetelmästä löytyy heikkouksia, on menetelmä helppo korvata turvallisemmalla ilman, että avaintenvaihtoprotokollan pohjaa tarvitsee määritellä uudelleen. ISAKMP on suunniteltu tukemaan turvallisuusassosiaatioiden luomista kaikille protokollapinon kerroksille, ja tämä osaltaan auttaa keskittämään turvallisuusassosiaatioiden hallintaa



Kuva 4.2: ISAKMP:n geneerinen otsikkokenttä [17]

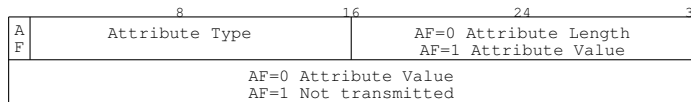


Kuva 4.3: Geneerinen payload-otsikkokenttä [17]

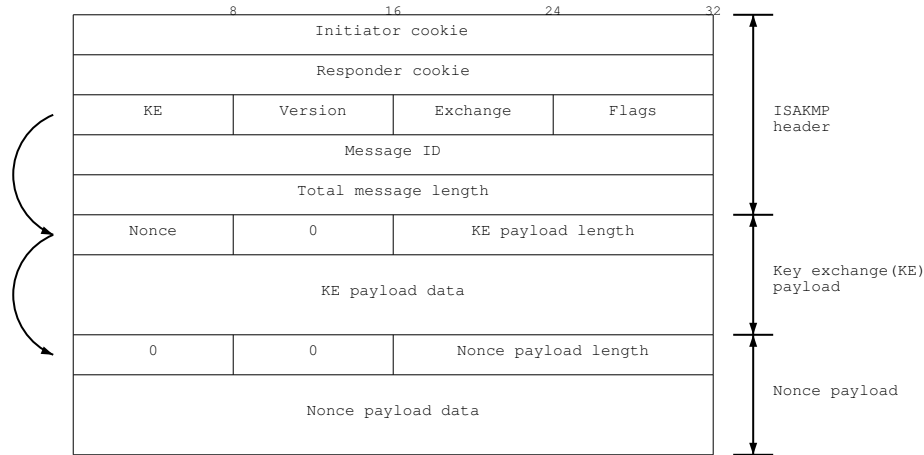
ja vähentämään tarvetta samojen toiminnallisuuksien implementoinnille useampaan paikkaan.

ISAKMP-paketin otsikkokenttä on esitetty kuvassa 4.2. *Initiator cookie* ja *responder cookie* -kentät eli piparit – joka neuvottelussa vaihtuvat satunnaisluvut – toimivat tunnistimina eri ISAKMP SA:iden välillä. Kumpikin osapuoli valitsee itse oman piparinsa, jolloin kentät toimivat suojana uudelleenlähetystä vastaan, koska vihamielinen kolmas osapuoli ei pysty häiritsemään liikennettä lähettämällä aikaisemmista yhteyksistä kaappaamiaan paketteja uudelleen. Lisäksi pipareita käytetään estämään DoS -hyökkäyksiä (Denial of Service) viivyttämällä paljon laskentatehoa vaativia toimintoja niin kauan kunnes piparit on vaihdettu. Täten vältetään käyttämästä laskentatehoa väärennettyihin paketteihin. *Next payload* -kenttä kertoo otsikkokenttää seuraavan kuormakentän tyyppin. *Major version* ja *minor version* -kenttien avulla erotetaan eri ISAKMP-versiot. *Exchange type* -kenttä kertoo minkä tyyppinen ISAKMP-vaihto on kyseessä, IPsec-järjestelmässä tämä on tyyppiä 2 eli identity protection. *Flags* -kenttä sisältää pakettiin liittyvää ylimääräistä tietoa. Määriteltynä ovat salauksesta kertova, turvallisuusassosiaatioiden muodostamisen synkronoiva sekä autentikoinnista kertova optio. *Message ID* -kenttää käytetään piparien ohella tunnistamaan oikea protokollayhteys. *Message length* kertoo koko paketin pituuden otsikkokenttä sekä kaikki kuormakentät mukaanluettuna.

Erilaisia kuormakenttiä on määriteltä kolmetoista. Kaikki ISAKMP-kuormakentät alkavat samanlaisella otsikkokentällä joka on esitetty kuvassa 4.3. Kuten ISAKMP-paketin otsikkokentässä, myös kuormakentän otsikkokentässä on seuraavan kuormakentän tyyppin kerto-



Kuva 4.4: Attribuutit [17]



Kuva 4.5: ISAKMP payloadien ketjutus [2, s. 105]

va kenttä, *next payload*. Seuraavat kahdeksan bittiä on varattu mahdollisille laajennuksille tulevaisuudessa. *Payload length* -kenttä kertoo kuormakentän pituuden otsikkokenttä mukaanluettuna.

Eräisiin kuormakenttiin on mahdollista lisätä data-attribuuttikenttiä lisäinformaation välittämiseksi. ISAKMP ei määrittele data-attribuuttikenttien sisältämää tietoa, vaan sen voi suojauksen tarjoava protokolla määrittellä itse. Esimerkiksi sovittaessa tiivistesumman laskevasta tai salauksen suorittavasta algoritmista, käytetään data-attribuuttikenttää välittämään tuetut algoritmit yhteyden muodostajalta vastaanottajalle. Vastaavasti vastaanottaja ilmoittaa valitsemansa algoritmit data-attribuuttikentissä. Data-attribuuttikenttä on esitetty kuvassa 4.4.

ISAKMP-paketit rakentuvat edellä selostettujen ohjeiden mukaan otsikkokentästä, halutusta määrästä kuormakenttiä, sekä mahdollisista kuormakenttien sisältämistä data-attribuuttikentistä. Ensimmäisen kuormakentän tyyppi ilmoitetaan otsikkokentässä ja seuraavat kuormakenttien otsikkokentissä kuvan 4.5 osoittamalla tavalla.

Otsikkokenttien muoto on kiinteä. Tällä on haettu yksinkertaisuutta pakettien parsimisen implementoivaan osaan muilta osin erittäin monimutkaiseksi muodostuvassa ohjelmistossa.

## 4.1.2 IPSec DOI

ISAKMP määrittelee miten neuvotellaan, mutta Domain of Interpretation for ISAKMP -dokumentti määrittelee miten neuvotellaan turvallisuusassosiaatio juuri IPSec:in käyttöön. Dokumentissa kerrotaan nimeämiskäytäntö neuvoteltaville protokollille, neuvoteltavat parametrit ja muut vastapuolelle välitettävät protokollaspesifiset tiedot. [2]

RFC2408:ssa on listattu vaatimukset, joita ISAKMP asettaa DOI-dokumentille. DOI:n pitää määrittellä nimeämiskäytäntö järjestelmään lisäämilleen protokollille sekä tarvittaessa tietoturvapoliitikat. Dokumentin pitää määrittellä tarvitsemansa SA-attribuutit, kuormakentät sekä ISAKMP-paketin tilanteen kuvaus -kenttä. Lisäksi tarvittaessa pitää esitellä uudet avaintenvaihtomenetelmät ja tiedonantoviestit.

## 4.1.3 Vaiheet

ISAKMP määrittelee kaksi erillistä neuvotteluvaihetta. Ensimmäisessä vaiheessa osapuolet muodostavat välilleen autentikoidun ja suojatun tiedonsiirtokanavan, IKE SA:n. Toisessa vaiheessa tätä kanavaa käytetään neuvotellessa tietoturvapalveluita muille protokollille. IKE SA tarjoaa autenttisuuden, eheyden ja luottamuksellisuuden, jonka suojassa toisen vaiheen neuvottelut suoritetaan. [2, s. 105, 106]

Vaiheen kaksi seurauksena syntyviä turvallisuusassosiaatioita luodaan ja tuhoetaan tarpeen mukaan, yleensä avaimen eliniän tultua täyteen, mutta IKE SA pysyy voimassa. Täten kahdella erillisellä vaiheella säästetään vaivaa ajan myötä, kun autentikointi tarvitsee suorittaa vain kerran. [2, s. 105, 106]

Laskentatehon säästämiseksi toisen vaiheen avaimet luodaan käyttäen siemenenä IKE SA:n salausavainta. Tämä voisi olla tietoturvariski jos IKE SA:n avain paljastuisi, koska tällöin voisi olisi mahdollista avata myös kaikkien toisen vaiheen seurauksena syntyneiden turvallisuusassosiaatioiden liikenne. Tätä varten toisen vaiheen neuvottelussa on mahdollista valita PFS-optio (Perfect Forward Secrecy), jolloin kaikki toisen vaiheen turvallisuusassosiaatioiden avaimet luodaan alusta alkaen Diffie-Hellman -menetelmällä. [2, s. 105, 106]

#### 4.1.4 Vaihdot

IKE määrittelee viisi erilaista viestien vaihtoa tai moodia eri tilanteisiin. Kolme näistä ovat turvallisuusassosiaatioiden luomiseen. Ensimmäisen vaiheen suorittamiseen on kaksi moodia, *main mode* ja *aggressive mode*. Kummankin lopputuloksena on IKE SA. *Main mode* tarvitsee yhteensä kuusi viestiä; kaksi ensimmäistä neuvottelevat suojauspolitiikan, kaksi seuraavaa vaihtavat Diffie-Hellman -arvot avaimen sopimiseksi sekä satunnaisluvut, kaksi viimeistä autentikoivat Diffie-Hellman -vaihdon. [3] Valittu autentikointimenetelmä vaikuttaa viestien rakenteeseen, mutta ei niiden järjestykseen.

*Aggressive mode* on nopeampi tapa neuvotella IKE SA, joka saavutetaan rajoittamalla neuvottelumahdollisuuksia. Ensimmäisessä viestissä aloittaja lähettää listan mahdollisista suojausmenetelmistä, Diffie-Hellman -arvonsa, satunnaisluvun sekä identiteettinsä. Vastaaja valitsee sopivan suojausmenetelmän ja lähettää sen takaisin oman Diffie-Hellman -arvonsa, satunnaislukunsa, identiteettinsä sekä autentikointikuormansa kera. [3]

*Aggressive mode* omaa huomattavasti suppeammat neuvottelumahdollisuudet nopeutensa vuoksi. Tätä moodia käytetään silloin, kun on hyvin tarkka tieto vastapuolen käyttämästä tietoturvapoliitikasta – esimerkiksi etätyöyhteys työntekijän kotoa työpaikalle. Lisäksi tämä moodi on toimintamekanisminsa vuoksi ainoa vaihtoehto silloin, kun halutaan käyttää etukäteen sovittua avainta autentikointimetodina ja yhteyden aloittajan osoitetta ei tiedetä etukäteen. Tällaisesta tilanteesta käytetään nimitystä ”Road Warrior”.

*Aggressive mode* paljastaa yhteyden salakuuntelijalle enemmän tietoa kuin *main mode* ja sitä pidetään tietoturvariskinä. Tämän takia IPSec -toiminnallisuuden linux-käyttöjärjestelmään tarjoava FreeS/WAN -projekti [20] ei ole implementoinut *aggressive mode:a* omaan toteutukseensa.

Toisen vaiheen suorittaa *quick mode*. Lopputuloksena on IPSec SA. Kuten aikaisemmin on mainittu, *quick mode* on suojattu IKE SA:lla, joten kaikki paketit ovat salattuja ISAKMP-otsikkokentän jälkeen. Tämä moodi vaatii kolme viestiä: Aloittaja lähettää viestin autentikoivan ja uudelleenlähetysyökkäyksen estävän tiivisteen, listan mahdollisista suojausmenetelmistä ja satunnaisluvun. Aloittaja voi lähettää myös Diffie-Hellman -arvonsa, halutesaan PFS:n käyttöön. Vastaaja lähettää tiivistefunktion, valitsemansa suojausmenetelmät, satunnaisluvun sekä Diffie-Hellman -arvonsa siinä tapauksessa että aloittaja lähetti oman-

sa. Viimeinen paketti on aloittajan kuittaus saatuaan vastaajan paketin.

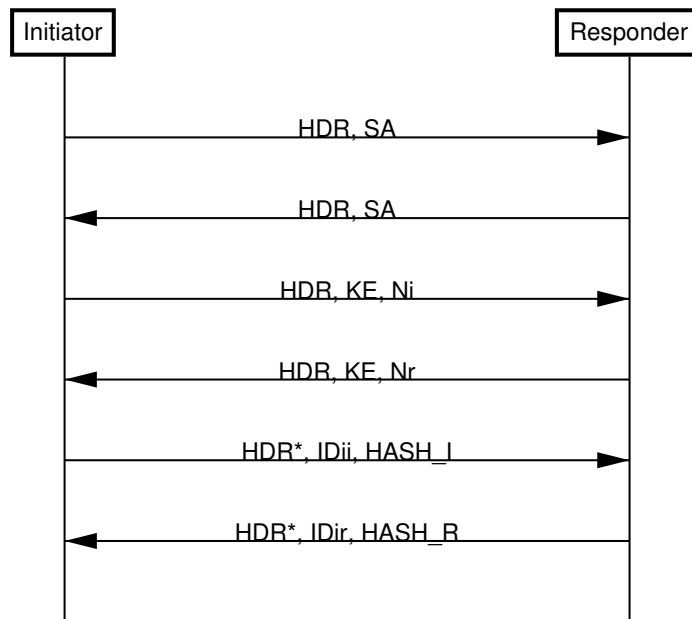
*New group mode:a* voidaan käyttää haluttaessa neuvotella uusi Diffie-Hellman -ryhmä. Jos mikään viidestä valmiista Diffie-Hellman -ryhmästä ei kelpaa avaimen luomiseen, voidaan tämän moodin avulla sopia vastapuolen kanssa omat parametrit vaihtamalla yhden viestin. Tätä moodia voi käyttää vain ensimmäisen vaiheen suorittamisen jälkeen, joten IKE SA:n on käytettävä jotain valmista ryhmää.

Lisäksi IKE määrittelee tiedotusviestin *informational exchange*, jonka avulla voidaan ilmoittaa turvallisuusassosiaation tuhoamisesta tai virhetilanteista. Tiedotusviestiin ei lähetetä kuittausa. IKE:n määritelmä ei vaadi tiedotusviestien käyttöä, vain suosittelee. Tämän takia toisen osapuolen ei voi olettaa ymmärtävän viestien sisältöä ja niistä saatava hyöty jää pieneksi. Jos IKE SA on luotu, lähetetään tiedotusviesti sen suojassa, muuten viesti kulkee selväkielisenä.

#### 4.1.5 Autentikointimenetelmät

Jotta yhteyden salaamisesta voidaan olettaa olevan hyötyä, pitää vastapuolen identiteetti olla tiedossa. IKE tarjoaa neljä erilaista keinoa autentikoitua vastapuolelle ensimmäisen vaiheen neuvottelujen aikana: digitaalinen allekirjoitus, kaksi julkisen avaimen menetelmää ja etukäteen sovittu avain. Nämä menetelmät ovat käytössä sekä main- että aggressive-moodissa. Autentikointimenetelmä vaikuttaa viestien salaukseen ja autentikointiin tarkoitettujen avaimien luomistekniikkaan, eheyden varmistavan tiivistesumman laskemiseen sekä viestien sisältöön. Viestien tarkoitus ja järjestys kuitenkin pysyvät samana riippumatta autentikointimenetelmästä. Tässä eri menetelmien yhteydessä on esitelty vain yleisemmin käytetyn main moodin kulku. Salaus- ja autentikointiavainten luomisen ja aggressive moodin kulun selvittää RFC2409.

Aloittaja lähettää ensimmäisessä viestissään hänelle sopivat suojausmenetelmät. Samassa viestissä lähetetään myös ehdotus autentikointimenetelmäksi. Vastaaja valitsee hänelle sopivat menetelmän ja viestien vaihto jatkuu siitä riippuen. Etukäteen jaettua avainta käyttäen main moodi etenee kuvan 4.6 mukaisesti. Tähdellä merkityt paketit ovat salattuja merkistä lähtien.



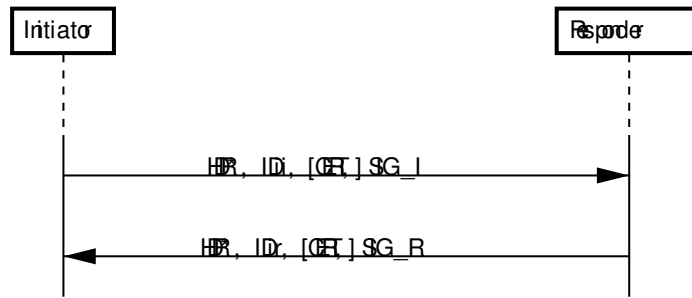
Kuva 4.6: Main moodi käytettäessä etukäteen sovittua avainta [3]

*HDR* on ISAKMP-otsikko, *SA* on suojaustekniikan neuvotteluun käytettävä security association payload, *KE* on Diffie-Hellman -avaintenvaihdossa käytettävä key exchange payload, *Ni* ja *Nr* ovat aloittajan ja vastaajan valitsemat satunnaisluvut, *IDii* ja *IDir* ovat identiteetit ja *HASH\_I* ja *HASH\_R* ovat avaimelliset tiivistesummat.

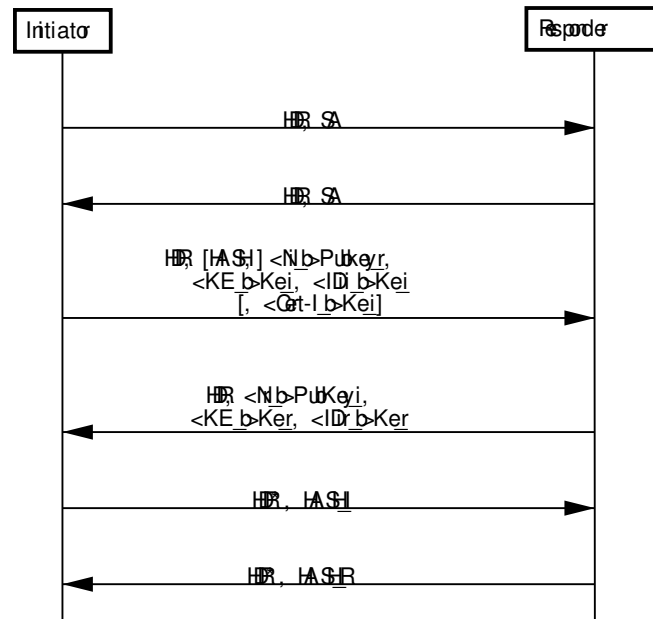
Koska osapuolten identiteetti kulkee viimeisessä viestissä salattuna ja salausavaimen luomiseen tarvitaan tieto vastapuolen identiteetistä, pitää vastapuoli tunnistaa IP-osoitteen perusteella jotta osataan käyttää oikeaa etukäteen sovittua avainta. Vastapuolen IP-osoitteen pitää olla tiedossa, joten tämä menetelmä ei sovi road warrior -tilanteeseen, vaan pitää käyttää aggressive moodia.

Julkisen avaimen menetelmiä käytettäessä pitää kummallakin osapuolella olla vastapuolen julkinen avain tiedossaan. Digitaalista allekirjoitusavainta käyttäen neuvottelu etenee kuvan 4.7 mukaisesti. Kuvassa on esitettyä vain kaksi viimeistä viestiä, muilta osin viestit ovat samat kuin käytettäessä etukäteen sovittua avainta. Hakasulkeilla merkityt kentät eivät ole pakollisia.

*SIG\_I* ja *SIG\_R* ovat aloittajan ja vastaanottajan allekirjoitukset. Osapuolten on mahdollista lähettää sertifiikaatteja allekirjoituksensa autenttisuuden toteamisen helpottamiseksi. Allekirjoitus tehdään edellisessä menetelmässä esiintyneen tiivistesumman yli.



Kuva 4.7: Main moodi käytettäessä digitaalista allekirjoitusta [3]



Kuva 4.8: Main moodi käytettäessä uudistettua julkisen avaimen menetelmää [3]

Myös julkisen salausavaimen menetelmää käytettäessä pitää vastapuolen julkinen avain olla tiedossa. Alkuperäinen menetelmä vaati kaksi julkisen avaimen salausoperaatiota kummaltakin osapuolelta. Lisäksi se ei sallinut sertifiikaattien lähettämistä toiselle osapuolelle oman identiteetin paljastumatta. Mahdollisuus lähettää sertifiikaatteja vastapuolelle on ratkaiseva suuremmissa järjestelmissä, jos sertifiikaattien reaaliaikaisen noutamisen mahdollistavaa järjestelmää ei ole käytössä. Uudistettu menetelmä vähentää julkisen avaimen salausoperaatiot puoleen ja mahdollistaa sertifiikaattien lähettämisen anonyymisti. Uudistetun julkisen avaimen menetelmän toimintaperiaate on esitetty kuvassa 4.8.

Aloittajan toisen viestin sisältämä satunnaisluku  $Ni\_b$  on salattu käyttäen vastaajan julkista avainta. Muut kentät on salattu käyttäen symmetristä salausavainta, joka saadaan laskemalla tiivistefunktio jaetusta salaisuudesta ja satunnaisluvuista  $Ni\_b$  ja  $Nr\_b$ . Vastaajan pitää en-

sin purkaa satunnaisluvun salaus käyttäen omaa salaista avaintaan, selvittää symmetrinen avain satunnaisluvun avulla ja tämän jälkeen purkaa loput kentät. Aloittaja tekee samoin saatuaan vastaajan toisen paketin.

#### 4.1.6 Algoritmeista sopiminen

IKE:n tarjoamat neuvottelumahdollisuudet molemmille osapuolille sopivien algoritmien löytämiseksi ovat erittäin monipuoliset. Neuvotteluun käytetään turvallisuusassosiaatio-kuormakenttää (Security Association payload, SA payload). Vaihtoehtoja luetellessaan aloittaja voi luoda hyvin monimutkaisen loogisista AND- ja OR-operaattoreista koostuvan rakenteen, joka sisältää ehdotuksia (Proposal) ja muunnoksia (Transform).

SA-kuormakenttä voi sisältää useita ehdotuksia. Ehdotuksilla on numerot, jotka ilmaisevat loogisia operaatioita. Jos ehdotuksilla on eri numerot, luetaan se OR-operaatioksi niiden välillä. Sama numero kahdella tai useammalla ehdotuksella luetaan niiden väliseksi AND-operaatioksi. Yksi ehdotus voi sisältää useita muunnoksia, joiden välinen operaatio on aina OR. Kuvassa 4.9 on esitetty tilanne, jossa on neljä eri ehdotusta. Ensimmäinen ehdotus sisältää AH-algoritmeja, toinen ja kolmas ESP-algoritmeja ja neljäs sisältää pak-

```
Ehdotus 1: AH
  Muunnos 1: HMAC-SHA
  Muunnos 2: HMAC-MD5

Ehdotus 2: ESP
  Muunnos 1: 3DES ja HMAC-SHA
  Muunnos 2: 3DES ja HMAC-MD5

Ehdotus 3: ESP
  Muunnos 1: 3DES ja HMAC-SHA
  Muunnos 2: 3DES ja HMAC-MD5

Ehdotus 3: PCP
  Muunnos 1: LZS
  Muunnos 2: Deflate
```

Kuva 4.9: Turvallisuusassosiaation neuvottelu

kaus algoritmeja. Koska kahdella viimeisellä ehdotuksella on sama numero, luetaan niiden välille AND-operaatio. Tämän yhdistelmän sekä muiden välillä on OR-operaatio. Koko rakenne olisi ((AH-HMAC-SHA or AH-HMAC-MD5) or (3DES HMAC-SHA or 3DES HMAC-MD5) or [(3DES HMAC-SHA or 3DES HMAC-MD5) and (PCP-LZS or PCP-DEFLATE)]). Vastaaja valitsee itselleen sopivan suojausmenetelmän ja lähettää vain sen takaisin omassa SA-kuormakentässään.

## 4.2 IKEv2

Nimensä mukaisesti IKEv2 on kehitetty IKE:n pohjalta. IKE:stä saatujen kokemusten perusteella uudessa versiossa on palvelunestohyökkäyksien varalta suojauduttu huolellisemmin ja protokollaa on kevennetty vähentämällä modulaarisuutta ja neuvottelumahdollisuuksia.

### 4.2.1 Muutokset vanhasta versiosta

IKEv2 -määrittelydokumentti *draft-ietf-ipsec-ikev2-05.txt* listaa uudelle versiolle seuraavat tavoitteet:

1. Määritellä koko protokolla yhdessä dokumentissa aikaisemman kolmen sijaan. Tämä koskee myös NAT-yhteensopivuutta, laajennettua autentikointia ja etäosoitteen noutamista määritteleviä laajennuksia.
2. Yksinkertaistaa protokollaa korvaamalla kaikki aikaisemmat ensimmäisen vaiheen moodit yhdellä menetelmällä. Autentikointimenetelmä ei myöskään vaikuta enää kuin yhden kuormakentän sisältöön.
3. Poistaa sekaannusta aiheuttavat turhat kentät otsikkokentästä.
4. Nopeuttaa protokollan toimintaa lyhentämällä transaktio neljään viestiin sekä yhdistämällä ensimmäisen IPSec SA:n neuvottelu ensimmäisen vaiheen neuvotteluun.
5. Muuttaa IKE SA:n suojaus ESP:n kaltaiseksi implementoinnin ja turvallisuusanalyysin helpottamiseksi.
6. Selkeyttää protokollaa ja vähentää mahdollisia virhetiloja lisäämällä olennaisille paketeille kuittaus sekä lisäämällä paketteihin sarjanumero.

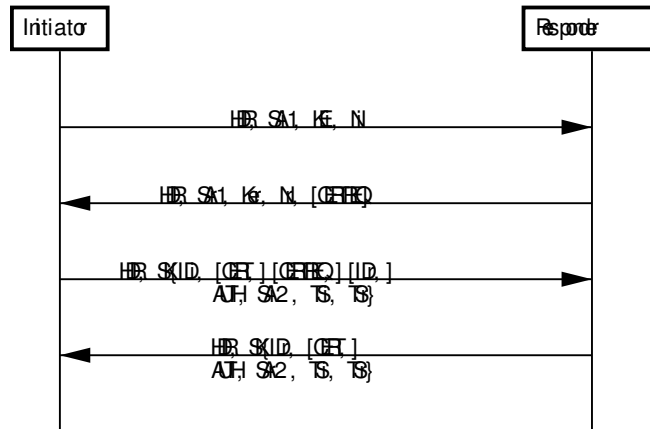
7. Parantaa protokollan vakautta siten, että vastaaja ei suorita merkittävää laskentatehoa vaativia operaatioita ennen kuin aloittaja on todistanut vastaavansa oikeasta IP-osoitteesta. Vastaajan ei myöskään tarvitse tehdä tilasiirtymää ennen kuin aloittaja on autentikoinut itsensä.
8. Korjata tietoturva-aukkoja.
9. Lisätä suojattavan liikenteen määritteleville liikenteen valitsimille (Traffic Selector) oma kuormakenttä, mikä sallii joustavamman määrittelyn.
10. Korvata monimutkainen algoritmien neuvottelumahdollisuus kiinteillä valmiiksi määritellyillä vaihtoehdoilla (Suites).
11. Määritellä virhetilanteista palautuminen, jotta uusien protokollaversioiden määrittely olisi mahdollista rikkomatta yhteensopivuutta vanhojen versioiden kanssa.
12. Yhdistää ideat NAT:in määrittelydokumentista [22], jotta IKE voi neuvotella NAT-reitittimistä huolimatta.
13. Selventää miten pitää toimia verkkokatkoksen tai palvelunestohyökkäyksen tapahduttua.

Samalla on pyritty mahdollisimman paljon säilyttämään ensimmäisen version syntaksia ja määrittelyjä, jotta vanhat toteutukset voisi helpommin muuttaa tukemaan uutta versiota protokollasta.

#### 4.2.2 Ensimmäinen vaihe

IKEv2 käyttää edeltäjänsä tapaan kahta erillistä vaihetta. Vaihtoja on kuitenkin tehostettu ja yksinkertaistettu. Yleisimmän tapauksen – vain yhden IPSec SA -parin luomisen – nopeuttamiseksi ensimmäisen vaiheen vaihdon yhteydessä on mahdollista neuvotella ensimmäiset toisen vaiheen turvallisuusassosiaatiot. Tämän seurauksena ensimmäisen ja toisen vaiheen välinen raja on hämärtynyt ja määrittely puhuukin ”initial” ja ”CREATE\_CHILD\_SA” -vaihtoista. Ensimmäisen vaiheen toiminta on esitetty kuvassa 4.10.

Ensimmäinen viesti sisältää otsikkokentän *HDR*, aloittajan tukemat algoritmit *SAI1*, Diffie-Hellman -arvon *KEi* sekä SPI:nä käytettävän ’satunnaisluvun’ *Ni*. Vastaaja lähettää takaisin valitsemansa algoritmit *SAr1*, oman Diffie-Hellman -arvonsa *KEr* sekä oman SPI:nsä *Nr*. Lisäksi vastaaja voi pyytää tietyn sertifikaattiorganisaation varmentamaa sertifikaattia



Kuva 4.10: IKEv2, ensimmäinen vaihe [21, s. 7-8]

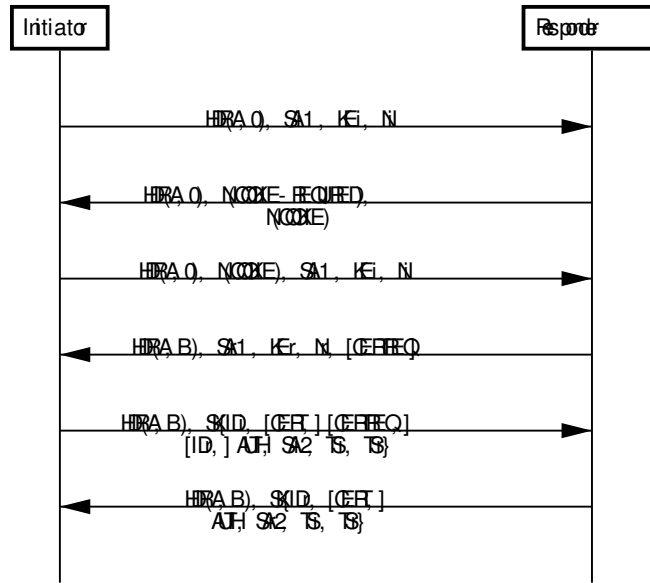
*CERTREQ*-kuormakentällä. Kuten IKEv1:ssäkin, symmetrisen salausavain *SK* lasketaan syöttämällä tiivistefunktiolle jaettu salaisuus ja satunnaisluvut.

Kolmannessa viestissä aloittaja lähettää symmetrisellä salausavaimella *SK* salattuna oman identiteettinsä, kaksi ensimmäistä viestiä autentikoivan tiivistesumman *AUTH* sekä arvot *SAi2* *TSi* ja *TSr*, jotka neuvottelevat IPsec SA:n parametrit. Lisäksi salattuna voi kulkea aloittajan sertifikaatti *CERT*, *CERTREQ* sekä vastapuolen identiteetti *IDr*. Vastapuolen identiteetti on tarkoitettu tilanteisiin, joissa useammilla identiteeteillä on sama IP-osoite. Tällöin vastapuoli tietää, minkä identiteetin kanssa yhteys halutaan muodostaa.

Neljäs viesti sisältää *SK:lla* salattuna vastaajan identiteetin *IDr*, viestin autentikoivan *AUTH*-kentän, sekä IPsec SA:n neuvotteluun tarkoitetut *SAr2:n*, *TSi:n* ja *TSr:n*. Lisäksi vastaaja voi lähettää oman sertifikaattinsa.

Ensimmäisen vaiheen neuvottelu vaatii siis normaalissa tapauksessa neljä viestiä. Ensimmäinen viestipari, nimeltään ”IKE\_SA\_INIT”, neuvottelee käytettävät algoritmit, vaihtaa SPI:t ja suorittaa Diffie-Hellman avaimenvaihdon. Toinen viestipari, ”IKE\_AUTH”, autentikoi edelliset viestit, identifioi osapuolet, vaihtaa sertifikaatit ja luo ensimmäisen IPsec SA:n.

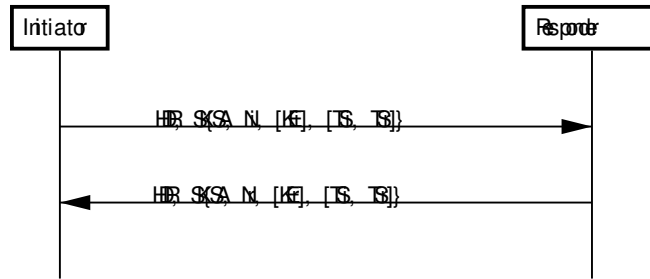
Jotta ensimmäinen vaihe normaalissa tapauksessa on saatu yksinkertaiseksi, on jouduttu tinkimään ominaisuuksista palvelunestohyökkäyksiä varten. Vastaajan on ensimmäisen viestin saatuaan pidettävä tallella protokollayhteyden liittyvää tilatietoa. Tätä ominaisuutta hyväksikäyttäen voidaan vastaajan muisti ehdyttää avaamalla runsaasti neuvotteluja saatta-



Kuva 4.11: IKEv2, ensimmäinen vaihe tilatonta piparia käyttäen[21, s. 18]

matta niitä kuitenkaan loppuun asti. Tämä ongelma on ratkaistu antamalla vastaajalle mahdollisuus vastata aloittajalle tilattomasti, vastaajan huomattessaan useita avoimia neuvotteluyhteyksiä. Vastaaja voi ensimmäisessä viestissään lähettää piparin, jonka se pystyy aloittajan vastatessa generoimaan täsmälleen samalla tavalla. Jos aloittajan lähettämä piparin on sama kuin uudelleengeneroitu, on aloittaja aktiivisesti neuvottelussa mukana ja voidaan edetä turvallisesti. Piparin voi generoida esimerkiksi laskemalla tiivistefunktion säännöllisesti vaihtuvasta avaimesta, aloittajan IP-osoitteesta ja SPI:stä sekä avaimen järjestysnumerosta. Ensimmäisen vaiheen neuvottelu, vastaajan käyttäessä piparia, on esitetty kuvassa 4.11.

Aloittajan ensimmäisen viestin jälkeen vastaaja laskee piparin arvon ja ilmoittaa tilattomasta toiminnastaan piparin kuormakentän edelle sijoitetulla COOKIE-REQUIRED -kuormakentällä. Aloittaja lähettää ensimmäistä viestiään vastaavan viestin, johon on liittänyt saamansa piparin arvon. Saatuaan oikean piparin arvon sisältävän viestin, vastaaja voi varmistua aloittajan olevan aktiivisesti mukana vaihdossa ja valitsee tässä vaiheessa myös oman SPI-arvonsa, kuten käy ilmi otsikkokentän perään liitettyistä merkinnöistä.



Kuva 4.12: IPsec SA:n luominen toisen vaiheen vaihdossa [21, s. 9]

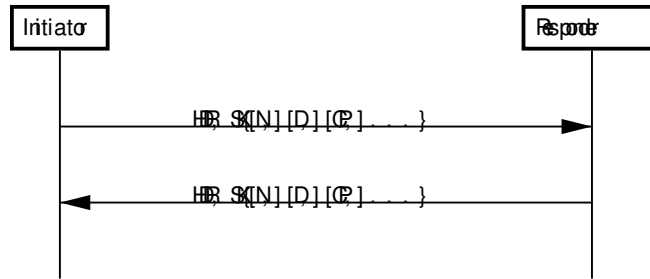
### 4.2.3 Toinen vaihe

IKEv2 määrittelee kaksi toisen vaiheen vaihtoa, IPsec SA:n luomiseen (CREATE\_CHILD\_SA Exchange) ja tiedonantoon (Informational Exchange). Kummatkin vaihdot ovat kahden viestin mittaisia ja kulkevat IKE SA:n suojassa, kun mahdollista. IPsec SA:n luominen on esitetty kuvassa 4.12.

CREATE\_CHILD\_SA -vaihto on aina suojattu symmetrisellä salausavaimella *SK*. Aloittaja lähettää turvallisuusassosiaation luomiseen tarvittavat parametrit *SA*, joka sisältää aloittajan tukemat algoritmit ja *Ni:n*, joka sisältää aloittajan valitseman SPI:n. Halutessaan PFS-ominaisuuden, aloittaja lähettää myös uuden Diffie-Hellman -arvon. Tässä yhteydessä aloittajalla tarkoitetaan toisen vaiheen vaihdon aloittajaa. Ensimmäisen vaiheen rooleilla ei ole tässä vaiheessa merkitystä. Vastaaja lähettää takaisin samanlaisen viestin hyväksymillään parametreilla.

Toisen vaiheen neuvottelua käytetään myös vaihdettaessa IKE SA:n avaimia. Tällöin neuvotellaan uusi IKE SA vanhan suojassa ennen sen sulkemista. Käytettäessä toisen vaiheen neuvottelua tähän tarkoitukseen, jätetään SPI:n ilmoittava kenttä tyhjäksi. Kaikki vanhan IKE SA:n alaisuudessa olevat IPsec SA:n siirtyvät uuden IKE SA:n alaisiksi. Kumpi tahansa osapuoli voi aloittaa toisen vaiheen neuvottelun halutessaan luoda uuden IPsec SA:n tai vaihtaa IKE SA:n avaimet.

Tiedonantovaihtoa käytetään virhetilanteista ilmoittamiseen, lisäinformaation ja konfiguraatietiedon välittämiseen ja turvallisuusassosiaation tuhoamiseen. Koska sivullisille halutaan antaa mahdollisimman vähän tietoa, on luonnollista lähettää tiedonantoviestit salatuna. Tiedonantoviestit suojataan niitä vastaavan ensimmäisen vaiheen turvallisuusassosi-



Kuva 4.13: IKEv2:n tiedonantovaihto [21, s. 11]

aatiolla. On kuitenkin kaksi tilannetta, jolloin suojaaminen ei ole mahdollista. Jos vastaaja hylkää aloittajan lähettämän ensimmäisen vaiheen ensimmäisen viestin, ei turvallisuusassosiaatiota ole vielä luotu. Toinen tapaus koskee koneen uudelleenkäynnistämistä; jos vastaanotetaan IPSec-paketti tuntemattomalla SPI-numerolla, on kyseessä todennäköisesti vanha turvallisuusassosiaatio, jonka vastapuoli luulee vielä olevan käytössä. Tällöin lähetetään tiedonantoviesti, joka kulkee suojaamattomana. Jos vastapuoli, saatuaan tällaisen suojaamattoman tiedonantoviestin, tuhoaisi turvallisuusassosiaation, olisi kolmannen osapuolen helppo viestejä väärentämällä vaikeuttaa viestinvälitystä. Tämän takia suojaamaton tiedonantoviesti pitää ottaa kehoituksena tarkistaa vastapuolen tilanne, eikä luottaa siihen kuten suojattuun viestiin. Tiedonantoviestiin lähetetään aina kuittaus, joten tiedonantovaihto koostuu yhdestä viestiparista kuvan 4.13 mukaisesti.

Tiedonantoviesti koostuu tiedotus-, poisto- ja konfiguraatio-kuormakentistä. Erikoistapauksena on viesti, jossa ei ole yhtään kuormakenttää, jota käytetään testaamaan toisen osapuolen olemassaolo. Tiedotus-kuormakenttä voi sisältää tietoa esimerkiksi tunnistamattomista kuormakentistä, väärästä SPI-arvosta tai implementaation tukemista valinnaisista ominaisuuksista. Poisto-kuormakenttää käytetään turvallisuusassosiaatioiden tuhoamiseen ja se sisältää tuhottavia turvallisuusassosiaatioita vastaavat SPI-arvot. Konfiguraatio-kuormakenttä on tarkoitettu tilanteisiin, jossa otetaan suojattu yhteys organisaation sisäverkkoon ja halutaan käyttää sisäverkon osoitteita. Tämän kuormakentän avulla voidaan pyytää muun muassa IPv4- tai IPv6-osoite, aliverkon maski, nimipalvelimen osoite ja muuta IP:n konfiguraatietoa.

Tiedotus- ja konfiguraatio-kuormakenttä voi esiintyä myös missä tahansa muussa IKEv2-viestissä tiedonantoviestin lisäksi.

#### 4.2.4 Algoritmeista sopiminen

Kryptografisista algoritmeista neuvottelua on huomattavasti yksinkertaistettu alkuperäiseen IKE:en verrattuna. IKE:n joustavat neuvotteluominaisuudet – jotka mahdollistavat erittäin monimutkaisen ehdotuksen – on IKEv2:ssa korvattu valmiiksi määritellyillä vaihtoehdoilla, joten IKEv2:en SA-kuormakenttä sisältää numeroituja ehdotuksia. Vastaaja valitsee yhden ehdotuksista ja palauttaa sen aloittajalle. *Draft-ietf-ipsec-ikev2-05.txt* määrittelee yhdeksän vaihtoehtoa, jotka on esitetty taulukossa 4.1.

Nämä algoritmit ovat vasta alustavia valintoja ja määrittely ei kehotakaan toteuttamaan juuri näitä, koska on hyvin todennäköistä että ne vaihtuvat vielä määrittelyprosessin aikana. Ne ovat kuitenkin suuntaa-antavan tarkastelun kannalta hyödyllisiä ja osoittavat IKE- ja ESP-algoritmien olevan pääosassa.

#### 4.2.5 Yhteensopivuus osoitteenmuunnoksen kanssa

NAT (Network Address Translation) ja NATP (Network Address and Port Translation) ovat tekniikoita, jotka ovat kehitetty ratkaisemaan IP-osoitteiden vähydestä johtuvat ongelmat. (Jatkossa käytetään nimitystä NAT kummastakin tekniikasta.) Vaikka Internet Protokollan versio 6 on kehitetty osaltaan juuri tämän ongelman ratkaisemiseksi, on NAT tullut IP-maailmaan jäädäkseen. Osaltaan tämä johtuu siitä, että se parantaa jossain määrin NAT-reitittimen takana olevien koneiden tietoturvaa, koska niihin ei ole mahdollista ottaa yhteyttä osoitteenmuunnoksen takana olevilta koneilta. Suuri osa kotitalouksiin tarkoitettuisista Internet-yhteyksistä käyttää tätä tekniikkaa ja tämän takia ipsec-työryhmä on halunnut kiinnittää huomiota IKEv2:n ja NAT:in yhteentoimivuuteen.

IKE:n ensimmäisen version määrittelyssä ei juurikaan ole mietitty, miten se toimii NAT:in läpi. Jälkikäteen tehtyjen määrittelyiden avulla on kuitenkin saatu aikaan osittainen toiminnallisuus. Näiden määrittelyiden pohjalta on IKEv2:n toiminnallisuuteen lisätty ominaisuuksia, jotka mahdollistavat lähes normaalin toiminnan NAT-reitittimen takaa. Yksi olennaisimmista muutoksista on IPSec-liikenteen kapselointi UDP-pakettien sisälle, jolloin NAT-reitittimen suorittamat osoitteen ja porttien muutokset vaikuttavat vain paketin uloimpaan kerrokseen jättäen IPSec:in varmentamat otsikkokentät ennalleen. Toinen muutos on sallia IKE-liikenteen lähdeportiksi mikä tahansa entisen portin 500 sijasta. Tämä helpottaa

Numero	Protokolla	Algoritmit
1	IKE	168-bittinen 3DES CBC, DH-ryhmä 2 (1024) HMAC-SHA1-96 eheys HMAC-SHA1 tiivistefunktio
2	IKE	168-bittinen 3DES CBC, DH-ryhmä 5 (1536) HMAC-SHA1-96 eheys HMAC-SHA1 tiivistefunktio
3	IKE	128-bittinen AES CBC, DH-ryhmä 5 (1536) HMAC-SHA1-96 eheys HMAC-SHA1 tiivistefunktio
4	IKE	128-bittinen AES CBC, DH-ryhmä 14 (2048) HMAC-SHA1-96 eheys HMAC-SHA1 tiivistefunktio
5	IKE	128-bittinen AES CTR, DH-ryhmä 14 (2048) AES-CBC MAC + XCBC eheys ja tiivistefunktio
1001	ESP	ei laajennettuja sekvenssinumeroita 3DES kolmella avaimella HMAC-SHA1-96 eheys
1002	ESP	laajennetut sekvenssinumerot 128-bittinen AES CBC HMAC-SHA1-96 eheys
1003	ESP	laajennetut sekvenssinumerot 128-bittinen AES CTR AES-CBC MAC + XCBC eheys
2001	AH	HMAC-SHA1-96 eheys

Taulu 4.1: IKEv2 algoritmivaihtoehdot [21, s. 41-42]

tilannetta, jossa kaksi NAT-reitittimen takana olevaa konetta liikennöivät saman ulkopuolisen koneen kanssa, koska NAT-reititin voi erottaa koneiden liikenteet toisistaan vaihtamalla lähdeosoitteen ja tekemällä osoitteenmuunnos- ja reitityspäätöksen porttinumeroon perustuen.

Eräät NAT-toteutukset on alkuperäisen IKE:n toiminnan helpottamiseksi konfiguroitu tunnistamaan porttiin 500 tuleva liikenne IPSec-liikenteeksi ja suorittamaan tämän perusteella erikoistoimintoja kuten osoitteenmuunnosta SPI-kenttien perusteella. Jotta vältettäisiin sekaannuksia muun muassa tällaisissa NAT-reitittimissä, on UDP-kapseloidun IPSec-liikenteen portiksi määrätty 4500.

Yhteyden aloittaja voi tunnistaa olevansa NAT-reitittimen takana käyttäen tietotuskuormakenttän tyyppejä ”NAT-DETECTION-SOURCE-IP” ja ”NAT-DETECTION-DESTINATION-IP”. Vastaaja täyttää nämä kentät vastaavilla osoitteilla ja verratessaan kenttien arvoa saapuneen paketin IP-otsikkokentässä oleviin arvoihin voi aloittaja tunnistaa matkan varrella tapahtuvan osoitteenmuunnoksen.

#### 4.2.6 Ulkoiset autentikointimenetelmät

Käytännössä voi joskus tulla vastaan tilanteita, jossa pitää käyttää jotain muuta autentikointikeinoa kuin sertifikaattia tai jaettua salaisuutta. Tällainen tilanne voi olla esimerkiksi silloin, kun halutaan autentikoida tietokoneen sijaan henkilö, joka aloittaa yhteyden. Henkilöllä voi olla hallussaan esimerkiksi kertakäyttöisiä salasanoja tai haaste-vaste -tyyppinen toimikortti. IKEv2:een on otettu mukaan yksi ensimmäiseen versioon suunnitelluista ulkoisista autentikointimeteodeista, pppext-työryhmän suunnittelema EAP [23] (Extended Authentication Protocol).

IKEv2-määrittely jättää EAP-autentikointimenetelmien määrittelyn omaan dokumenttiinsa (RFC2284) tyytyen vain mainitsemaan yleisimmät menetelmät. Koska IKEv2:lla on oma menetelmänsä, jolla osapuolet kertovat identiteettinsä, ei EAPin määrittelemiä keinoja identiteetin kertomiseen käytetä.

Halutessaan käyttää EAP-autentikointia, aloittaja kertoo kolmannessa viestissä identiteettinsä kuten normaalistikin, mutta ei lähetä autentikoivaa sertifikaattia tai tiivistesummaa.

Neljännessä viestissä vastaaja kertoo identiteettinsä ja todistaa sen sekä lähettää merkkijonon tulostettavaksi aloittajan ruudulle. Aloittaja voi vastata käyttäen vastaajan ehdottamaa menetelmää tai pyytää eri EAP-menetelmää. Vastaaja jatkaa protokollayhteyttä normaaliin tapaan IKE-neuvottelun neljännellä viestillä varmistuttuaan aloittajan autenttisuudesta.

## 4.3 JFK

JFK (Just Fast Keying) on toinen ipsec-työryhmän työn tuloksena syntyneistä vaihtoehtoista IKE:n seuraajaksi. Sen suunnitteluun on ryhdytty hyvin erilaisista lähtökohdista kuin IKEv2:en suunnittelussa.

### 4.3.1 Suunnitteluperiaatteet

JFK:n suunnittelussa tavoitteena olleet kahdeksan ominaisuutta on esitetty taulukossa 4.2. Näistä käy ilmi, että toteutuksen yksinkertaisuus ja tehokkuus on ollut suunnittelijoille tärkeää, koska protokollan turvallisuus on tietysti avaintenvaihtoprotokollan perusominaisuus ja JFK on suunniteltu periaatteella, että määrittelyn ollessa mahdollisimman yksinkertainen toteutuksesta on helpompi tehdä turvallinen ja yhteensopiva. Palvelunestohyökkäyksien ollessa nykyään valitettavan yleisiä niihin on varauduttu hyvin kattavasti. Ainoa normaali- muotoisen JFK:n tukema autentikointimenetelmä on autentikointi sertifikaatteja käyttäen.

JFK:n määrittely sisältää kaksi eri versiota protokollasta, JFKr ja JFKi. Protokollat ovat hyvin samanlaisia. Ero on järjestyksessä, jossa osapuolet kertovat identiteettinsä vastapuolelle. Tällöin protokollat tarjoavat erilaisen suojan osapuolten identiteetin paljastumista vastaan. JFKr suojaa aloittajaa passiiviselta hyökkäykseltä ja vastaajaa sekä passiiviselta, että aktiiviselta hyökkäykseltä. JFKi suojaa aloittajaa aktiiviselta hyökkäykseltä, mutta vastaajan identiteettiä ei suojata ollenkaan. Tässä esitellään vain JFKr ja käytetään JFKr:stä nimitystä JFK, koska se on todennäköisempi vaihtoehto käytettäväksi protokollaksi sen identiteeteille tarjoaman paremman suojan vuoksi.

Suurin periaatteellinen ero JFK:n ja IKE-versioiden välillä on JFK:n yksivaiheisuus. Protokollan suunnittelijoiden mielestä kaksivaiheisuudella saavutettavat edut eivät riitä oikeutta-

Turvallisuus	Luodun avaimen pitää olla kryptografisesti turvallinen
Yksinkertaisuus	Mahdollisimman yksinkertainen
Muisti-DoS	Immuuni muistin ehdyttämistä vastaan
Laskenallinen-DoS	Immuuni laskentatehon ehdyttämistä vastaan
Yksityisyys	Osapuolten identiteetit pysyvät salassa
Tehokkuus	Protokollan pitää olla tehokas laskutehon, kaistanleveyden ja viestien määrän suhteen
Neuvottelemattomuus	Ei monimutkaisia ominaisuuksien neuvotteluja
PFS	Perfect Forward Secrecy -ominaisuus

Taulu 4.2: JFK:n suunnitteluperiaatteet [24]

maan siitä koituvaa raskautta ja monimutkaisuutta.

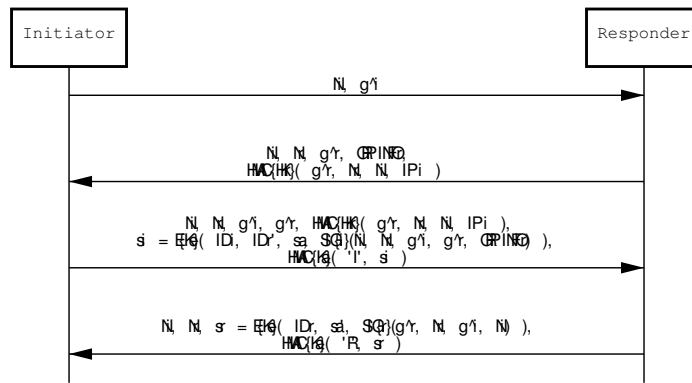
### 4.3.2 Toiminta

Protokollan toiminta on esitetty kuvassa 4.14.

Koko protokollayhteys käsittää neljä viestiä. Ensimmäisessä viestissä aloittaja lähettää satunnaisluvun sekä oman Diffie-Hellman -arvonsa.

Vastaaja lähettää oman satunnaislukunsa ja Diffie-Hellman -arvonsa, tukemansa Diffie-Hellman -ryhmät sekä viestin autentikoivan tiivistesumman. Tiivistesumman laskemisessa käytetty avaimen  $HKr$  tietää vain vastaaja, joka käyttää tiivistesummaa estämään uudelleenlähetyshyökkäykset.

Kolmannessa viestissä aloittaja joutuu lähettämään tiivistesumman todistaakseen olevansa aktiivisesti mukana avaintenvaihdossa. Aloittaja lähettää myös identiteettinsä ( $IDi$ ), ehdottamansa kryptografiset parametrit ( $sa$ ), sekä digitaalisen allekirjoituksensa, jotka kaikki on salattu Diffie-Hellman -arvoista luodulla symmetrisellä salausavaimella,  $Ke$ :llä. Digitaalisen allekirjoituksen avulla vastaaja voi varmistua aloittajan identiteetin olevan  $IDi$ -kentässä ilmoitettu. Lisäksi viesti sisältää Diffie-Hellman -arvoista luodulla avaimella,  $Ka$ :lla, luo-



Kuva 4.14: Just Fast Keying -protokollan toiminta [24]

dun tiivistesumman, joka varmistaa viestin lähettäjäksi sen osapuolen, jonka kanssa Diffie-Hellman vaihto juuri käytiin.

Viimeisessä, neljännessä, viestissä vastaaja lähettää  $Ke$ :llä salattuna oman identiteettinsä, turvallisuusassosiaatioon liittyvät parametrit sekä digitaalisen allekirjoituksensa. Kuten kolmannen viesti, tämäkin sisältää  $Ka$ :n avulla luodun tiivistesumman viestin autentikointiin.

Tilanteen vaatiessa vastaaja voi lähettää hylkäysviestin toisen tai neljännen viestin sijasta. Toisen viestin kohdalla tämä tulee kyseeseen silloin, kun aloittajan lähettämä Diffie-Hellman -ryhmä ei sovi vastaajalle. Protokollan yksinkertaisuudesta johtuen tällöin aloittaja aloittaa protokollavaihdon uudelleen alusta. Neljäs viesti voi olla hylkäysviesti, jos aloittaja ei ole autentikoinut itseään oikealla tavalla tai aloittajan ehdottamat turvallisuusassosiaation parametrit eivät sovi vastaajalle. Jälkimmäisessä tapauksessa vastaajan hylkäysviesti sisältää parametrit, jotka hänelle sopisivat. Neljännen viestin ollessa hylkäysviesti, aloittajalle riittää lähettää kolmas viestinsä uudelleen siten, että hylkäyksen aiheuttanut kohta on korjattu. Tämän jälkeen vastaaja lähettää neljännen viestinsä normaalisti ja turvallisuusassosiaatio on luotu.

### 4.3.3 Ominaisuudet

JFK:n suunnitteluperiaatteet ovat hyvin poikkeavat IKE-versioihin nähden. Samaan lopputulokseen – IPsec turvallisuusassosiaation luomiseen – päästään hyvin erilaisilla keinoilla. Nämä keinot ilmenevät protokollien erilaisina ominaisuuksina viestien vaihdon, tilakoneen monimutkaisuuden, vaadittavan laskentatehon ja autentikointimenetelmien suhteen.

JFK:n transaktio koostuu neljästä viestistä. Viestien kiinteä määrä helpottaa toteutusta tilakoneiden osalta sekä virhetilanteiden sattuessa niistä toipumisessa. Sekä aloittajan että vastaajan identiteetti on suojassa passiiviselta hyökkäykseltä. Aktiivisella hyökkäyksellä voi aloittajan identiteetin selvittää, koska aloittaja identifioi itsensä ensin. [24]

Palvelunestohyökkäyksien varalle on varauduttu huolellisesti; aloittajan on oltava viestienvaihdossa mukana yksi yhteyskierros ennen kuin vastaajan pitää suorittaa työläitä laskuoperaatioita. Lähettäessään toisen viestin vastaajalla ei ole vielä mitään tietoa aloittajan autentisuudesta, joten siinä vaiheessa vastaajan ei pidä joutua tekemään tilasiirtymää eikä tuhlaamaan juurikaan prosessoriaikaa. Vastaaja joutuukin tässä vaiheessa vain laskemaan tiivistefunktion. Kolmatta viestiä käsitellessään vastaajan pitää taas laskea tiivistefunktio, ja jos tulos täsmää viestissä tulleen tiivistesumman kanssa, laskemaan useita julkisen avaimen operaatioita. Tässä vaiheessa vastaajan voisi huijata kuluttamaan prosessoritehonsa lähettämällä vanhoja paketteja, jolloin vastaaja laskisi operaatioita turhaan. Tämän estääkseen vastaaja tallentaa lähettämänsä neljännen viestin. Tällöin vastaaja ei kuluta prosessoritehoansa julkisen avaimen operaatioihin vaikka duplikaatteja kolmannen vaiheen viestejä saapuisikin, koska viesti voidaan lähettää suoraan muistista.

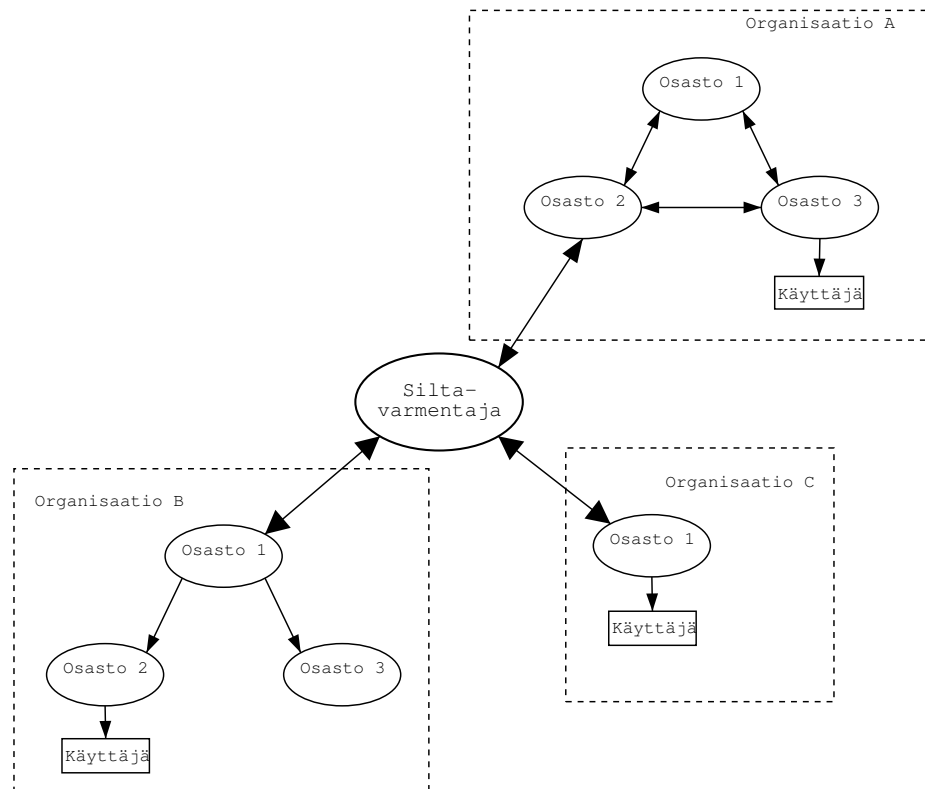
Normaalissa toimintamoodissaan JFK yksinkertaisuuden vuoksi käyttää autentikointiin ainoastaan sertifikaatteja. Protokollaa voidaan käyttää myös kevyessä moodissa (lightweight mode), jolloin autentikointi etukäteen jaettua avainta käyttäen on mahdollista. Kevyttä moodia voidaan käyttää myös haluttaessa perusprotokollaa laskentatehollisesti kevyempi keino uudistaa avain. Kevyessä moodissa autentikointiin käytetään digitaalisen allekirjoituksen ja julkisen avaimen operaatioiden sijaan tiivistefunktiota, jonka laskemiseen käytetään vaihtoehtoisesti joko ennalta sovittua tai edellisen protokollayhteyden aikana sovittua avainta.

Neuvottelumahdollisuudet on karsittu minimiinsä; aloittaja voi joko hyväksyä vastaajan hyväksymät algoritmit ja parametrit, tai aloittaa protokollayhteyden uudestaan. Tämä on seurausta suunnittelijoiden ajattelutavasta, jonka mukaan vastaaja tarjoaa palvelua ja voitaten yksipuolisesti määrätä haluamansa ominaisuudet. [24]

## 5 Julkisten avainten jakelu

Jotta julkisen avaimen käyttöön perustuvat autentikointimenetelmät voisivat käytännössä toimia, tarvitaan yhteisesti sovittu menetelmä, jolla toisten osapuolten julkisia avaimia saadaan omaan haltuun. Tällaista järjestelmää kutsutaan julkisen avaimen infrastruktuuriksi (Public Key Infrastructure, PKI). Yleensä PKI määritellään järjestelmänä, johon kuuluu turvallinen menetelmä avainten jakeluun, hakemisto avainten säilytykselle ja noutamiselle, mekanismi julkisen avaimen peruuttamiselle sekä mahdollisuus luottamusketjujen rakentamiseen [25].

Julkisen avaimen infrastruktuurin keskeisimmät osapuolet ovat varmentajat, varmennettavat ja käyttäjät. Varmentaja (Certification Authority, CA) takaa, että varmennettavalla on hänen esittämänsä julkista avainta vastaava yksityinen avain, sekä varmistuu hänen henkilöllisyydestään. Käyttäjä luottaa varmentajaan, ja täten voi käyttää varmennettavan julkista avainta heidän väliseensä autentikointiin. Varmentajien määrästä ja heidän välisistään suhteista riippuen PKI-järjestelmälle on kehitelty erilaisia hierarkioita. Todennäköisimmin yleistyy järjestelmä, jossa eri organisaatiot itse toimivat varmentajana jäsenilleen ja organisaatioiden välinen varmentaminen annetaan erityisille siltavarmentajille, kuten on esitetty kuvassa 5.1. Siltavarmentajat vähentävät huomattavasti ristiinvarmennusten määrää järjestelmässä, koska jokainen organisaatio tekee ristiinvarmennuksen vain siltavarmentajan kanssa. Tämä järjestelmä on siitä hyvä, että organisaatioiden ei niin halutessaan tarvitse olla riippuvaisia kolmannelta osapuolelta organisaation sisäisten sertifikaattien muodostamisessa. Tällainen järjestelmä on käytössä muunmuassa Yhdysvaltojen hallituksen virastojen välisessä PKI:ssä (The Federal Bridge CA Project) [15].

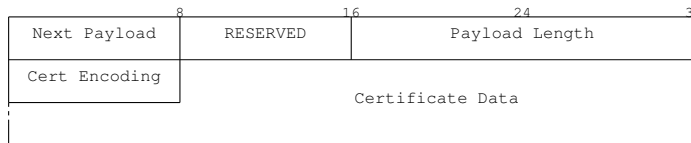


Kuva 5.1: Organisaatioiden PKI-järjestelmien yhdistäminen siltavarmentajan avulla [15, s. 65]

Kuten PKI:n määritelmässä sanottiin, pitää järjestelmässä olla keino turvallisesti jakaa avaimet. Tämä tarkoittaa sitä, että avaimia ei siirron aikana pystytä muuttamaan ja avain on todella sen osapuolen, jonka sen väitetään olevan. X.509 -sertifikaatteja käytettäessä sertifikaatti itsessään sisältää eheyden ja autenttisuuden varmistavan digitaalisen allekirjoituksen, jolla nämä ominaisuudet saavutetaan. On kuitenkin menetelmiä, jossa julkiset avaimet jaetaan pelkältään, toisinsanoen ilman kolmannen osapuolen allekirjoittamaa digitaalista allekirjoitusta. Tällöin pitää olla jokin mekanismi, jolla avaimen eheydestä ja autenttisuudesta voidaan varmistua. Yksi tällainen järjestelmä on Opportunistic Encryption, joka käyttää avainten suojaamiseen ja niiden alkuperästä varmistumiseen nimipalvelun DNSSEC -tietoturvalaajennuksia.

## 5.1 Certificate Payload

Koska IKE:ä käyttävät osapuolet ovat yhteydessä toisiinsa reaaliaikaisesti, toisin kuin esimerkiksi sähköpostisovelluksia käytettäessä, on osapuolten mahdollista lähettää oma serti-



Kuva 5.2: Certificate Payload [17, s. 33]

Certificate Type	Value
NONE	0
PKCS #7 wrapped X.509 certificate	1
PGP Certificate	2
DNS Signed Key	3
X.509 Certificate - Signature	4
X.509 Certificate - Key Exchange	5
Kerberos Tokens	6
Certificate RevocationList (CRL)	7
Authority RevocationList (ARL)	8
SPKI Certificate	9
X.509 Certificate - Attribute	10
RESERVED	11 - 255

Kuva 5.3: Certificate Type -kentän arvot [17, s. 34]

fikaattinsa salattua yhteyttä luotaessa. IKE ei siis välttämättä tarvitse ulkoista sertifikaattihakemistoa ja protokollaa sertifikaattien jakelulle. IKE:n suunnittelussa tapahtuneista virheistä johtuen tämä ei kuitenkaan aina pidä paikkaansa. Erityisesti, julkisen salausavaimen avulla autentikoiduttaessa pitää vastapuolen julkisen avaimen olla tiedossa etukäteen. Koska reaaliaikainen protokolla kuitenkin mahdollistaa sertifikaattien lähettämisen yhteyden luomisen yhteydessä, on IKEv2:ssa pyritty korjaamaan edellisen version virheet ja parannettu sertifikaattien lähettämiseen liittyviä ominaisuuksia.

ISAKMP:n käyttämä certificate payload on esitetty kuvassa 5.2. *Certificate Encoding* -kenttä määrittää *Certificate Data* -kentän sisältämän sertifikaatin tyyppin. Kuvan 5.3 taulukko osoittaa eri tyyppjä olevan runsaasti, mutta käytännössä vain X.509 -sertifikaatit ovat käytettyjä.

Certificate Payload -kuormakenttää vastaavan Certificate Request Payload -kuormakentän avulla voi vastapuolelle ilmoittaa lähettäjän luottamista varmentajista. Tällöin ei välttämättä tarvitse lähettää sertifikaattiketjua koko pituudeltaan, vaan vain lähettäjän luottamusankkurista (jokin sertifikaatti luottamusketjun varrella, jonka oikeellisuuteen suoraan luotetaan) lähtien. Kuormakenttä on hyödyllinen myös silloin, kun osapuolilla on useamman varmen-

tajan myöntämiä sertifikaatteja, joista tämän kuormakentän avulla osataan valita oikea.

## 5.2 Opportunistic Encryption

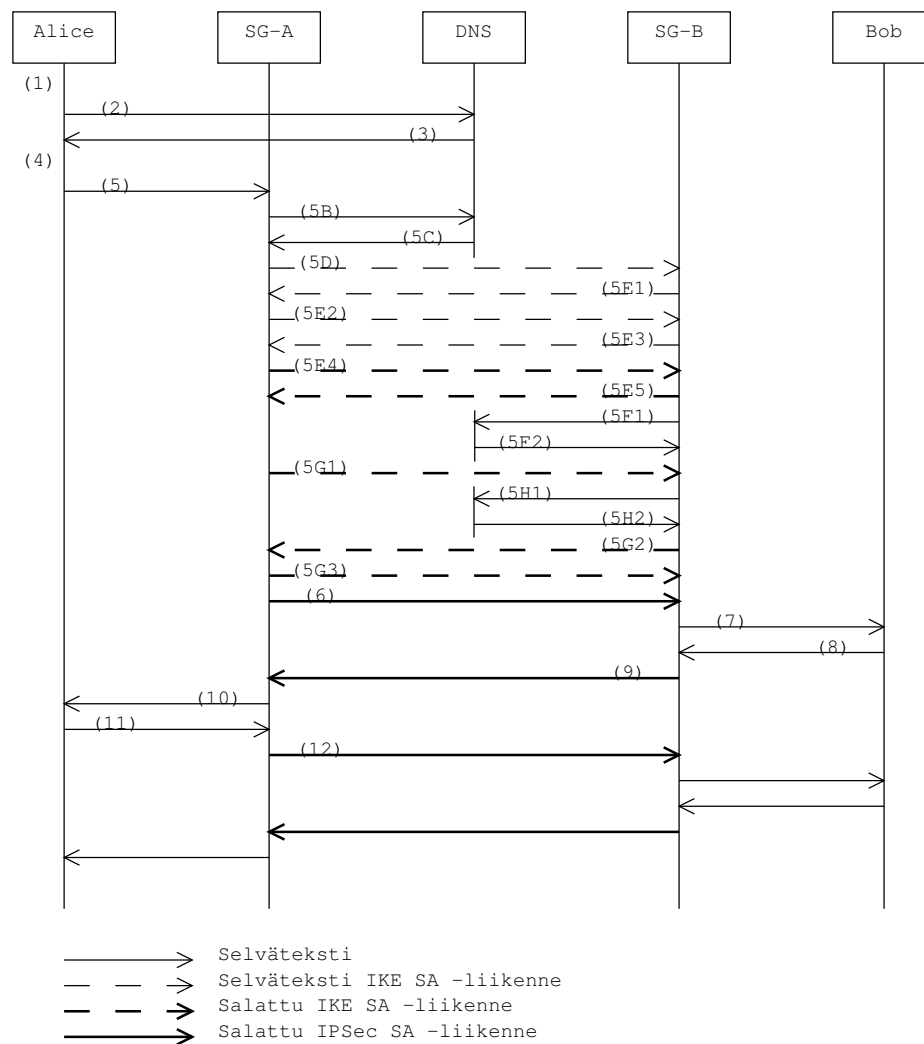
Yleisen PKI-järjestelmän hitaan edistymisen vuoksi FreeS/WAN-ohjelmiston tekijät ovat kehittäneet uuden menetelmän jakaa autentikointiin vaadittavia julkisia avaimia. Ajatuksena on ollut käyttää jo olemassa olevia tekniikoita mahdollisimman vähin muutoksin, jotta tämän uuden tekniikan käyttöönotto olisi mahdollisimman helppoa ja mahdollista suurelle osalle potentiaalisista IPSec-järjestelmän käyttäjistä. Opportunistic encryption -nimellä (OE) [26] kulkeva menetelmä käyttää nimipalvelua (Domain Name System, DNS) autentikointiavainten jakamiseen. Nimipalvelua sinällään ei ole suunniteltu tietoturvaa silmälläpitäen, ja sitä vastaan suunnatuilla aktiivisilla hyökkäyksillä OE-järjestelmän turvallisuus voidaan helposti romahduttaa jakamalla vääriä autentikointiavaimia väärennetyissä nimipalveluvastauksissa. Tämän estämiseksi OE-järjestelmä vaatii kryptografisesti suojatun nimipalvelun (DNS Security Extensions, DNSSEC). Opportunistic encryption -järjestelmä tarvitsee myös toimivan käänteisnimipalvelun tarkistaakseen tietoturvareitittimen oikeuden reitittää liikennettä tiettylle työasemalle. Käyttäjä ei kuitenkaan usein itse voi vaikuttaa oman osoitteensa käänteisnimipalvelun toimivuuteen, vaan asia on hänen palveluntarjoansa vastuulla. Kaikki palveluntarjoajat eivät ole hoitaneet käänteisnimipalvelua kunnolla, mikä on toinen OE-järjestelmän heikko kohta.

### 5.2.1 Toiminta

Jotta työasema A voisi käyttää opportunistic encryption -järjestelmää, pitää sen IP-osoitetta vastaavassa käänteisnimipalvelun TXT-kentässä olla työaseman käyttämän tietoturvareitittimen osoite ja julkinen avain (kuva 5.4). TXT-kenttä on tekstimuotoinen, ja se voi sisältää yleistä tietoa osoitteen haltijasta. Tässä tapauksessa kenttä sisältää peräkkäin tietoturvareitittimen osoitteen ja julkisen avaimen. Jos työasema B haluaa ottaa yhteyden työasema A:han, tietää B:n tietoturvareititin TXT-kentän perusteella ottaa yhteyden A:n tietoturvareitittimeen ja varmistua sen autentisuudesta. Hyvän yleiskuvan järjestelmän toiminnasta antaa esimerkkitapaus, joka on esitetty kuvassa 5.5 ja etenee seuraavasti (SG-A ja SG-B ovat A:n ja B:n tietoturvareitittimet):

### X-IPsec-Server(P)=A.B.C.D KEY

Kuva 5.4: Työasema A:n TXT-kenttä käänteisnimipalvelussa [26, s. 26]



Kuva 5.5: Esimerkki OE-järjestelmän toiminnasta [26, s. 37]

1. Käyttäjä tai sovellus päättää ottaa yhteyden koneeseen B.
2. Käyttöjärjestelmä lähettää nimipalvelukyselyn.
3. Vastaus kyselyyn saapuu ja käyttöjärjestelmä palauttaa kysyttyä DNS-nimeä vastaavan IP-osoitteen sovellukselle.
4. Sovellus aloittaa TCP- tai UDP-yhteyden avaamisen.
5. Tietoturvareititimet luovat välilleen tunnelin:
  - a) SG-A saa B:lle osoitetun paketin ja tallettaa sen välimuistiinsa.
  - b) SG-A kysyy nimipalvelusta B:n osoitetta vastaavaa TXT-tietuetta.
  - c) SG-A saa vastauksen nimipalvelukyselynsä ja tietää SG-B:n olevan B:n tietoturvareititin.
  - d) SG-A aloittaa IKE:n ensimmäisen vaiheen neuvottelun SG-B:n kanssa.
  - e) IKE:n ensimmäisen vaiheen neuvottelu suoritetaan loppuun.
  - f) SG-B kysyy nimipalvelusta A:n osoitetta vastaavaa TXT-tietuetta varmistuakseen SG-A:n olevan A:n tietoturvareititin.
  - g) Suoritetaan IKE:n toisen vaiheen neuvottelu.
  - h) SG-B tekee nimipalvelukyselyn.
6. SG-A lähettää välimuistiin tallennetun paketin.
7. SG-B saa paketin ja lähettää sen B:lle purettuaan salauksen ja varmistuttuaan paketin eheydestä.
8. B lähettää vastauspaketin jonka SG-B vastaanottaa.
9. SG-B lähettää paketin eteenpäin SG-A:n kanssa neuvoteltua tunnelia pitkin.
10. SG-A purkaa salauksen, varmistuu paketin eheydestä ja välittää sen A:lle.
11. A vastaanottaa paketin ja lähettää uuden paketin B:lle.
12. SG-A vastaanottaa paketin ja lähettää sen eteenpäin käyttäen valmiiksi neuvoteltua tunnelia.

### 5.2.2 Kryptografisesti suojattu nimipalvelu, DNSSEC

Kuten viimeaikaiset hyökkäykset Internetin juurinimipalvelimia kohtaan ovat osoittaneet[27], nimipalvelun häiriötön toiminta on olennaisen tärkeää koko Internetin toiminnan kannalta. Nimipalvelu on kuitenkin suunniteltu aikana, jolloin Internet ei ollut vihamielinen ympäristö ja protokollia ja sovelluksia ei tarvinnut suunnitella äärimmäistä turvallisuutta silmälläpitäen. Niinpä, vaikka nimipalvelu onkin erinomaisen

onnistuneen kehittelyn tulos – sen skaalautuvuus Internetin suosion räjähdysmäisestä kasvusta huolimatta ei ole muodostunut rajoitteeksi missään vaiheessa – on turvallisuusnäkökohdat jätetty hyvin vähälle huomiolle. Kuka tahansa, joka pystyy kääntämään nimipalvelukyselyt omalle koneellensa, voi palauttaa kyselyihin virheellisesti omassa hallinnassaan olevia IP-osoitteita ja täten mahdollisesti esiintymään toisena palveluna, esimerkiksi nettipankkisivustona.

IETF:n DNS Extensions -työryhmä on perustettu parantamaan nimipalvelun turvallisuutta. Työskentelyn tuloksena on syntynyt DNSSEC-niminen määrittely [28], joka määrittelee eheyden ja tiedon lähteen autenttisuuden takaavat sekä julkisten avainten säilyttämisen ja jakelun mahdollistavat menetelmät. Nimipalvelutiedon autenttisuudesta ja eheydestä voidaan varmistua lähettämällä kyseisen hallinta-alueen yksityisellä avaimella salattu digitaalinen allekirjoitus vastauksen mukana. Koska nimipalveluhierarkian ylemmällä tasolla oleva taho varmentaa alapuolellansa olevan hallinta-alueen julkisen avaimen omalla yksityisellä avaimellaan, muodostuu varmenteista luottamusketju, jossa jokaisen nimipalveluasiakkaan tarvitsee suoraan luottaa vain hierarkian ylimpään tasoon.

## 5.3 LDAP

X.500 -standardin mukainen hakemisto on International Organization for Standardizationin (ISO) [29] määrittelemä erittäin monipuolinen hajautettu tietokanta. X.500 -hakemisto käyttää Directory Access Protocol:aa (DAP) tiedon noutamiseen palvelimilta asiakkaille ja Directory Service Protocol:aa (DSP) palvelimien väliseen tiedonsiirtoon. Laajuudesta ja monipuolisuudesta johtuen DAP -protokollan asiakasohjelma on usein liian raskas toteuttaa. Tämän johdosta alettiin protokollasta kehittämään kevyempää versiota, jota kutsutaan nimellä Lightweight Directory Access Protocol (LDAP) [30]. LDAP on tällä hetkellä vahvin ehdokas yhtenäisen PKI-järjestelmän hakemistoprotokollaksi. PKIX-työryhmä on RFC2587:ssä [31] määritellyt LDAPv2-protokollan käytön X.509-sertifikaattien noutamiseen.

LDAP:ia on DAP:iin verrattuna kevennetty muun muassa siirtämällä se toimimaan suoraan TCP:n (Transmission Control Protocol) päällä, kun DAP käytti OSI-protokollamallia. Lisäksi protokollaelementtejä on koodattu merkkijonoiksi aikaisemman binäärikoodauksen

sijaan. Myös BER (Basic Encoding Rules) on kevennetty versio DAP:in käyttämästä.

X.500-juuristaan johtuen LDAP käyttää hakemisto-objektien määrittelyyn Abstract Syntax Notation number One:a (ASN.1) [32]. PKIX-työryhmän kirjoittama RFC2587 määrittelee PKI-järjestelmän vaatimien objektien esitystavat ASN.1-muodossa.

## 5.4 Muita keinoja

Sertifikaattien jakeluun on ehdotetty myös eräitä yleisesti käytössä olevia protokollia. Tällaisia ovat File Transfer Protocol (FTP) ja Hypertext Transfer Protocol (HTTP). Etuna näillä protokollilla on se, että käytännössä jokainen Internetissä kiinni oleva tietokone käyttöjärjestelmästä ja laitteistosta riippumatta osaa niitä. Kyseisiä protokollia käytettäessä sertifikaattien pitäisi sisältää CRL:n ja sertifikaattien julkaisupaikan kertova URL-kenttä, jotta tiedettäisiin ottaa yhteys oikeaan palvelimeen rakennettaessa luottamusketjuja ja tarkistettaessa sertifikaatin pätevyys. Jos hakemiston käyttäjien autentikointi ei ole tarpeellista, riittää FTP-protokolla anonymikäyttäjänä kirjautuen. HTTP-protokollan avulla on mahdollista myös autentikoida käyttäjät SSL- tai TLS-protokollaa käyttäen.

IPSec:in käyttöön näitä protokollia ei ole vakavasti harkittu. Koska näitä protokollia ei alunperin ole suunniteltu hierarkisen hakemiston yhteysprotokollaksi, ei niillä ole siihen tarvittavia ominaisuuksia. Ne eivät myöskään ole laajennettavissa autentikointiominaisuuksien suhteen kuten esimerkiksi LDAP.

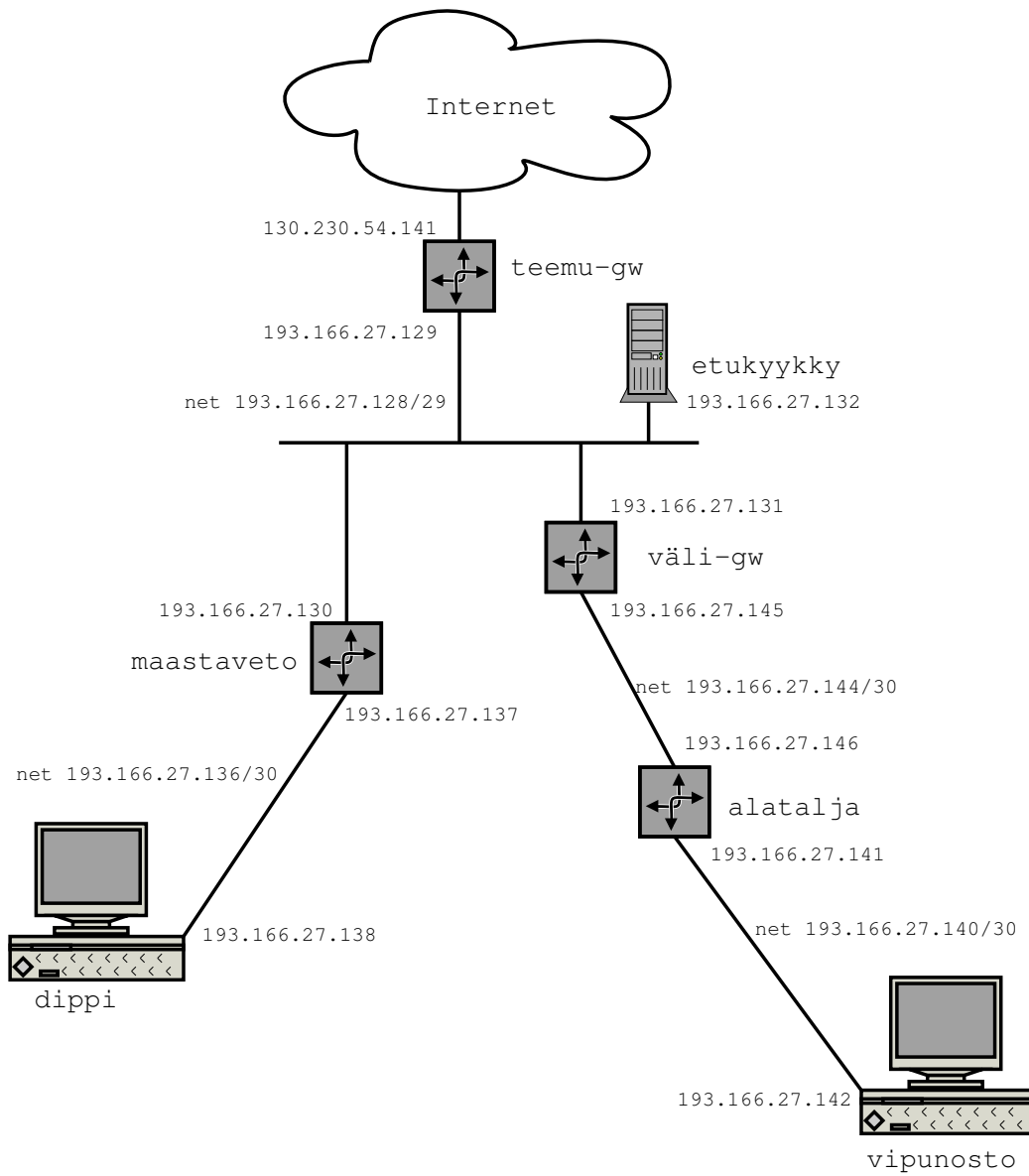
## 6 Käytännön testaus

Käytännön testeissä haluttiin saada käytännön kokemuksia eri menetelmien toiminnasta. Koska IKE:n seuraajan valitseminen on tätä kirjoitettaessa vielä kesken, ei implementaatioita niistä vielä ole saatavilla. Määrittelyprosessin aikana monet erittäin olennaisetkin ominaisuudet ovat muuttuneet draftin edellisestä versiosta, ja täten alustavien implementaatioiden tekeminen olisikin turhaa. Testiverkon käytössä keskityttiinkin tutkimaan erilaisten avaintenjakelumenetelmien toimivuutta IKE:n tämänhetkisen version yhteydessä.

Eri menetelmien hyvien ja huonojen puolien selvittämiseen ja käytännön toiminnan testaamiseen käytettiin kuvan 6.1 mukaista testiverkkoa.

Testiverkon reitityksessä käytetään OSPF-reititysprotokollaa (viite RFC 1247). Reitittimet *vali-gw* ja *teemu-gw* ovat Ciscon valmistamia ja tietoturvareitittimet *maastaveto* ja *alatalja* 200MHz Pentium Pro PC -koneita. Tietoturvareitittimillä ajetaan Zebra -reititysohjelmistoa [33], käyttöjärjestelmänä *Debian sarge* [34] tai *RedHat 7.3* [35] tilanteesta riippuen. Aliverkkojansa edustavat työasemat *dippi* ja *vipunosto* ovat PC-koneita, käyttöjärjestelmänä *Debian sarge*. *Etukyykky* toimii testiverkon nimi- ja LDAP-palvelimena ja *vipunostolla* on asennettuna FTP-palvelin. Tietoturvareitittimillä on käytetty *Ethereal*-verkkoanalysointia [36] liikenteen kaappaamiseen.

IPSec-implemентаationa käytettiin FreeS/WAN -ohjelmistoa. FreeS/WAN on avoimeen lähdekoodiin perustuva linux-käyttöjärjestelmälle tarkoitettu IPSec-toteutus, joka sisältää sekä IKE-avaintenvaihtoprotokollan että IPSec'in tietoturva-protokollat.



Kuva 6.1: Menetelmien testauksessa käytetyn koeverkon topologia

No.	Time	Source	Destination	Protocol	Info
1	0.000000	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
2	0.005190	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
3	0.058052	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
4	0.122169	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
5	0.085411	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
6	0.060912	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
7	0.083127	193.166.27.130	193.166.27.146	ISAKMP	Quick Mode
8	0.119314	193.166.27.146	193.166.27.130	ISAKMP	Quick Mode
9	0.190159	193.166.27.130	193.166.27.146	ISAKMP	Quick Mode
10	2.271024	193.166.27.130	193.166.27.147	ESP	ESP (SPI=0x77489100)
11	0.002341	193.166.27.146	193.166.27.130	ESP	ESP (SPI=0x77489100)

Kuva 6.2: Verkkoliikenne Certificate Payload -kenttää käytettäessä

## 6.1 Oman sertifi kaatin lähettäminen

Oman sertifi kaatin lähettäminen protokollayhteyden aikana testattiin käyttäen IKE:n *Certificate Payload* -kenttää. *Maastaveto* ja *alatalja* toimivat tietoturvareitittiminä takanaan oleville työasemille. Tietoturvareitittimet oli konfiguroitu siten, että ne muodostavat välilleen suojatun tunnelin vain suojatakseen työasemien *dippi* ja *vipunosto* välillä kulkevan liikenteen. Liikenteen generoiminen suoritettiin hakemalla tiedosto *vipunostolla* olevalta FTP-palvelimelta käyttäen FTP-protokollaa.

Yhteyden datagrammien vaihto on esitetty kuvassa 6.2. Kuvassa näkyy pakettien lähettämisen välillä kulunut aika sekä käytettävä protokolla. Neuvottelu sujuu kohtuullisen nopeasti; koko ensimmäisen vaiheen neuvottelu on suoritettu reilussa kolmessa sekunnin kymmenyksessä. Koska oma sertifi kaatti lähetetään protokollaviestien mukana, ei yhteyksiä muihin koneisiin tarvitse ottaa. Kaikki paketit kulkevat tietoturvareitittimien välillä. Tässä konfiguraatioissa käytössä ei ollut sertifi kaattien peruuttamiseen tarkoitettua CRL:ää.

Avaintenvaihtoprotokollan konfiguroiminen lähettämään oma sertifi kaatti on yksinkertaista ja useissa implementaatioissa oletusasetus. Täten ainoiksi monimutkaisemmiksi tehtäviksi jäävät tarvittavan sertifi kaatti-infrastruktuurin luominen ja oman sekä CA:n sertifi kaattien konfigurointi avaintenvaihtoprotokollaa toteuttavalle prosessille.

## 6.2 Nimipalvelu sertifi kaattien jakelumethodina

Nimipalvelu on valmiiksi olemassaoleva maailmanlaajuinen hajautettu tietokanta ja ajatus sen hyödyntämiseksi sertifi kaattien jakeluun on ollut usein esillä. Tässä testattiin

No.	Time	Source	Destination	Protocol	Info
1	0.000000	193.166.27.130	193.166.27.132	DNS	Standard query TXT 142.27.166.193.in-addr.arpa
2	0.000610	193.166.27.132	193.166.27.130	DNS	Standard query response TXT
3	0.004395	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
4	0.002871	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
5	0.056709	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
6	0.111531	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
7	0.373721	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
8	0.256905	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
9	0.066583	193.166.27.130	193.166.27.146	ISAKMP	Quick Mode
10	0.178220	193.166.27.146	193.166.27.130	ISAKMP	Quick Mode
11	0.325199	193.166.27.130	193.166.27.146	ISAKMP	Quick Mode
12	1.616643	193.166.27.130	193.166.27.147	ESP	ESP (SPI=0x77489100)
13	0.002372	193.166.27.146	193.166.27.130	ESP	ESP (SPI=0x77489100)

Kuva 6.3: Verkko liikenne *maastavedolla* Opportunistic Encryption -menetelmää käytettäessä

Opportunistic Encryption -nimellä tunnettua menetelmää selvittää verkkolaitetta vastaava tietoturvarvitin sekä noutaa tämän sertifikaatti. Testitilanne vastaa kuvan 5.5 esittämää tilannetta.

Tietoturvarvitimet *maastaveto* ja *alatalja* oli konfiguroitu siten, että kaikki niiden aliverkosta tuleva liikenne suojataan jos mahdollista. Käytännössä tämä tarkoittaa sitä, että reitittävän liikenteen tullessa reitittimelle, jos tälle ei ole vielä luotu turvallisuusassosiaatiota, se kysyy nimipalvelusta kohdeosoitetta vastaavaa TXT-tietuetta. Jos tietueessa on kerrottu tietoturvarvitin osoite, muodostetaan SA tämän tietoturvarvitin kanssa ja liikenne kohdeosoitteeseen reititetään luodun turvallisuusassosiaation läpi. Tällainen tapahtuma on yhteyden aloittajan tietoturvarvitineltä kaapattuna esitetty kuvassa 6.3.

Kaksi ensimmäistä pakettia ovat nimipalvelukysely, jossa selvitetään vastapuolen tietoturvarvitin, ja vastaus siihen. Muuten kaappaus näyttää pääpiirteittäin samalta kuin Certificate Payload -kenttää käytettäessä. Vastaanottajan tietoturvarvitineltä kaapatussa liikenteessä, kuvassa 6.4 näkyy suurempia eroja. *Alataljan* pitää myös selvittää *maastavedon* sertifikaatti, sekä tarkistaa että tämä tietoturvarvitin todellakin on valtuutettu toimimaan *dipin* liikenteen suojaajana.

Kaappauksessa näkyy, miten ennen ensimmäisen vaiheen viimeistä viestiä – siis heti kuin voidaan varmistua IKE-yhteyden aloittajan autenttisuudesta – tehdään nimipalvelukysely *maastavedon* IP-osoitetta vastaavasta KEY-tietueesta. Kun vastapuolen sertifikaatti on saatu vastaukseksi, ja todettu sen vastaavan vastapuolen ilmoittamaa identiteettiä, voidaan ensimmäinen vaihe suorittaa loppuun. Kun toisen vaiheen alussa *maastaveto* ilmoittaa haluavansa muodostaa IPsec SA:n *dipin* puolesta, tarkistetaan toisella kyselyllä *dipin* IP-osoitetta vastaavan TXT-tietueen ilmoittaman tietoturvarvitin olevan tämä reititin.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
2	0.001608	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
3	0.058100	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
4	0.109869	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
5	0.375527	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
6	0.004751	193.166.27.146	193.166.27.132	DNS	Standard query KEY 130.27.166.193.in-addr.arpa
7	0.003644	193.166.27.132	193.166.27.146	DNS	Standard query response KEY
8	0.246587	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
9	0.068617	193.166.27.130	193.166.27.146	ISAKMP	Quick Mode
10	0.044391	193.166.27.146	193.166.27.130	DNS	Standard query TXT 138.27.166.193.in-addr.arpa
11	0.004959	193.166.27.132	193.166.27.146	DNS	Standard query response TXT
12	0.126801	193.166.27.146	193.166.27.130	ISAKMP	Quick Mode
13	0.326737	193.166.27.130	193.166.27.146	ISAKMP	Quick Mode
14	1.616730	193.166.27.130	193.166.27.146	ESP	ESP (SPI=0x782c6e6c)
15	0.001266	193.166.27.146	193.166.27.130	ESP	ESP (SPI=0xbe50dc3e)

Kuva 6.4: Verkkoliikenne *alataljalla* Opportunistic Encryption -menetelmää käytettäessä

Toisen vaiheen neuvottelu on saatu päätökseen noin 1,4 sekunnin kuluttua. Tämä on jo huomattavasti – suunnilleen tuplasti – enemmän kuin Certificate Payload -kenttää käytettäessä. Toimintaa hidastavat useat nimipalvelukyselyt, jotka realistisemmassa verkossa usein vievät huomattavasti enemmän aikaa kuin tämän koeverkon tapauksessa. Lisäksi, Opportunistic Encryption -menetelmän seurakseen vaatima DNSSEC-mekanismi lisää nimipalvelukyselyiden viivettä entisestään.

## 6.3 LDAP sertifikaattien jakelumethodina

Lightweight Directory Access Protocol on yleisesti hyväksytty menetelmä säilyttää ja jakaa sertifikaattien peruutuslistoja (CRL), mutta sen käyttö julkisen avaimen sisältävän sertifikaattien jakeluun ei ole saanut suurta suosiota. Koska käytettävissä ei ollut implementaatiota, joka noutaisi sertifikaatit LDAP-hakemistosta, tässä testataan LDAP-hakemiston soveltumista reaaliaikaisen protokollan toimintaan käyttäen CRL:n hakemista hakemistosta julkisen avaimen sertifikaatin asemesta. Protokollan toimintamekanismin kannalta tällä ei ole eroa, koska CRL pitää noutaa samassa vaiheessa, kuin sertifikaatti noudettaisiin; ennen kuin voidaan varmistua toisen osapuolen autenttisuudesta. Myös jakelukanava voi olla samanlainen koska kumpikin, CRL ja julkisen avaimen sertifikaatti, on suojattu yksityisellä avaimella salatulla tiivistefunktiolla eli allekirjoituksella, ja täten kummankaan jakelukanavan itsessään ei tarvitse tarjota autenttisuutta.

Testiä varten verkon nimipalvelin, *etukyykky* toimi myös LDAP-palvelimenä. Palvelimelle oli konfiguroitu yksinkertainen hierarkia objectclass-tietueita, jossa ylimpänä oli organization-luokka ”dn: o=ttkk,l=tampere,c=fi”, tämän alapuolella organizationalUnit-

No.	Time	Source	Destination	Protocol	Info
1	0.000000	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
2	0.045329	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
3	0.127736	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
4	0.269627	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
5	0.960592	193.166.27.130	193.166.27.146	ISAKMP	Identity Protection (Main Mode)
6	0.073535	193.166.27.146	193.166.27.130	TCP	1056 > 389 [SYN] Seq=2141423260 Ack=0 Win=5840 Len=0
7	0.002087	193.166.27.132	193.166.27.146	TCP	389 > 1056 [SYN, ACK] Seq=2141423261 Ack=3271009421 Win=5840 Len=0
8	0.000480	193.166.27.146	193.166.27.132	TCP	1056 > 389 [ACK] Seq=2141423261 Ack=3271009421 Win=5840 Len=0
9	0.002118	193.166.27.146	193.166.27.132	LDAP	MsgId=1 MsgType=Bind Request
10	0.001989	193.166.27.132	193.166.27.146	TCP	389 > 1056 [ACK] Seq=3271009421 Ack=2141423275 Win=5792 Len=0
11	0.007993	193.166.27.132	193.166.27.146	LDAP	MsgId=1 MsgType=Bind Result
12	0.000227	193.166.27.146	193.166.27.132	TCP	1056 > 389 [ACK] Seq=2141423275 Ack=3271009435 Win=5840 Len=0
13	0.001392	193.166.27.146	193.166.27.132	LDAP	MsgId=2 MsgType=Search Request
14	0.006850	193.166.27.132	193.166.27.146	LDAP	MsgId=2 MsgType=Search Entry
15	0.000062	193.166.27.132	193.166.27.146	LDAP	MsgId=2 MsgType=Search Result
16	0.000271	193.166.27.146	193.166.27.132	TCP	1056 > 389 [ACK] Seq=2141423418 Ack=3271009973 Win=6432 Len=0
17	0.863534	193.166.27.146	193.166.27.130	ISAKMP	Identity Protection (Main Mode)
18	0.270278	193.166.27.130	193.166.27.146	ISAKMP	Quick Mode
18	0.134003	193.166.27.146	193.166.27.130	ISAKMP	Quick Mode
20	0.143826	193.166.27.130	193.166.27.146	ISAKMP	Quick Mode
21	0.362333	193.166.27.130	193.166.27.146	ESP	ESP (SPI=0x05b10997)
22	0.001626	193.166.27.146	193.166.27.130	ESP	ESP (SPI=0xe67c9f3f)

Kuva 6.5: Verkkoliikenne *maastavedolla* käytettäessä LDAP-palvelinta

luokka ”dn: ou=tl,t,o=ttkk,l=tampere,c=fi” ja tämän alapuolella cRLDistributionPoint-luokka ”dn: cn=testiverkko ca,ou=tl,t,o=ttkk,l=tampere,c=fi”. Koska implementaatio selvitti kyselyn juurikohdan sertifikaatissa ilmoitetun distinguished name -kentän ”cn=testiverkko ca,ou=tl,t,o=ttkk,l=tampere,c=fi” perusteella, kaikki kyselyt tehtiin tästä haarasta lähtien. Kysely pyysi kaikki objectclass-entryt, joissa on attribuuttina certificaterevocationlist tai authorityrevocationlist. LDAP-palvelimella oli ainoastaan yksi tämän haun parametrit täyttävä luokka, haluttu CRL, joka siis palautettiin vastauksessa. Kuvassa 6.5 on esitetty liikenne *maastavedolta* kaapattuna.

Kaappauksessa näkyy, miten ensimmäisen vaiheen neuvottelun viisi ensimmäistä pakettia vaihdetaan normaalisti. Tämän jälkeen avataan TCP-yhteys LDAP-palvelimelle suorittamalla normaali kolmitiekättely. Kolmitiekättelyn jälkeen muodostetaan yhteys LDAP-palvelua suorittavaan prosessiin bind-komennolla, johon saadaan palvelimelta vastaus. Seuraavaksi lähetetään haku, tässä tapauksessa CRL:stä, johon saadaan palvelimelta vastaukseksi yksi entry. Palvelin ilmoittaa haun päättymisestä search result -paketilla. Tämän jälkeen ensimmäisen vaiheen neuvottelu voidaan suorittaa loppuun ja aloittaa toisen vaiheen neuvottelu.

TCP-yhteyksien avaaminen voi viedä runsaasti aikaa. Varsinkin oikeassa ympäristössä LDAP-palvelin voi olla raskaasti kuormitettu sekä verkon topologiassa huomattavasti kauempana tietoturvarvitimmistä, jolloin viive voi kasvaa useita kertaluokkia suuremmaksi. Useissa peräkkäisissä kyselyissä kolmitiekättelyä ei kuitenkaan tarvitse tehdä joka kerta, vaan voidaan käyttää samaa yhteyttä. Käyttötarkoituksesta riippuen viive voi olla hyväksyttävä tai liian pitkä. Koeverkon tilanteessa toisen vaiheen neuvottelun loputtua aikaa oli kulunut noin kolme sekuntia.

Testiverkon tapauksessa tietoturva-asetitimet oli konfiguroitu muodostamaan yksi turvallisuusassosiaatio kahden aliverkon väliselle liikenteelle, jolloin yhteys muodostetaan heti ensimmäisen koneen liikennöidessä aliverkkojen välillä ja on näin valmiiksi luotuna muiden koneiden halutessa liikennöidä. Tällöin yhteys myös todennäköisemmin pysyy pidempään ylhäällä, eikä ajastuksesta johtuvia yhteyden alasajoja kerkiä tapahtumaan. Ympäristössä, jossa jokainen kone luo turvallisuusassosiaationsa itse, tämän kaltaiset viiveet eivät todennäköisesti olisi hyväksyttävissä. Keskitetty LDAP-tietokanta kuitenkin helpottaa sertifikaattien ylläpitoa ja tarjoaa näin huomattavia etuja skaalautuvuudessa.

## 7 Eri menetelmien analyysi

IETF:n toiminnan perustana on avoimuus. Kuka tahansa asiaan perehtynyt voi eri asioihin omistautuneiden työryhmien sähköpostilistoilla vaikuttaa standardointityöhön. Nämä listat ovat kaikille avoimia ja niiden seuraaminen auttaa ymmärtämään protokollan suunnittelun vaikeuksia ja syitä tehtyihin päätöksiin. Isec-työryhmän toiminnan seuraaminen on paljastanut myös komiteatyöskentelyn haittapuolet: suunnittelu voi joskus viedä huomattavasti arvioitua pidemmän ajan, kun yritetään löytää kaikkia osapuolia tyydyttävä ratkaisu. Samasta syystä tehdyt päätökset eivät aina ole käytännön kannalta parhaita, koska mukaan on lisättävä eri osapuolien vaatimia ominaisuuksia.

Tässä luvussa analysoin aikaisemmissa luvuissa esiteltyyn materiaaliin tukeutuen IKE:n ja sen seuraajien, JFK:n ja IKEv2:n, ominaisuuksia, heikkouksia ja vahvuuksia sekä selvittän suunnittelussa tehtyjen ratkaisuiden syitä. Luvussa myös analysoin autentikointiavainten jakelumenetelmiä teorian ja käytännön testien pohjalta, selvittäen niiden heikkoudet ja vahvuudet sekä soveliaimman ympäristön niiden käyttämiseen.

### 7.1 Avaintenvaihtoprotokollat

ISAKMP:n suunnittelijat aikanaan halusivat tehdä protokollasta mahdollisimman monipuolisen, että siitä hyötyisivät kaikki turvallisuusassosiaatioita tarvitsevat protokollat, eikä jäisi vain IPSec:in, suunnittelun motiivin, käyttöön. Ironisesti, ISAKMP:n monipuolisuuden mukanaan tuoma monimutkaisuus on kuitenkin ollut IKE:n suurin haittapuoli hidastaen

myös IPSec:in yleistymistä. Vaikka järjestetyt yhteensopivustestit ovat tilannetta hieman parantaneetkin, tälläkin hetkellä, haluttaessa muodostaa varmasti toimivia IPSec-yhteyksiä, on varmintä käyttää saman valmistajan tuotteita yhteyden molemmissa päissä.

Seuraavassa vertaillaan protokollia muutaman, perustavaa laatua olevan, ominaisuuden mukaan jaoteltuna.

### 7.1.1 Montako vaihetta

Avaintenvaihtoprotokollien fundamentaalinen ominaisuus on turvallisuusassosiaation luomiseen tarvittavien vaiheiden määrä. Toiset ovat valinneen yksinkertaisuuden skaalautuvuuden edelle ja luovat jokaisen turvallisuusassosiaation alusta alkaen, kun taas toiset luovat omansa varsinaisten käytettävien turvallisuusassosiaatioiden luomisen suojaamiseksi. Tämän ominaisuuden perusteella protokollaa kutsutaan yksi- tai kaksivaiheiseksi.

ISAKMP:n suunnittelussa on tehty valinta kaksivaiheisuuden hyväksi, mutta kokemuk- sista viisastuneena sille suunnitellut seuraajat toimivat hieman eri periaatteen mukaisesti. ISAKMP:n kaksivaiheisuudelle voi kuitenkin löytää useita perusteluita.

ISAKMP on alunperin suunniteltu siten, että useampi protokolla voisi käyttää sitä tur- vallisuusassosiaatioiden luomiseen. Tällöin kaksivaiheisuus on perusteltavissa sillä, että ISAKMP SA pitää luoda vain kerran, jonka jälkeen kaikki muiden protokollien SA:t voi- daan luoda suojattua yhteyttä käyttäen. Toisaalta, koska suurin osa protokollista kuitenkin kulkee IP-kerroksen päällä, ne voivat suoraan käyttää IPSec:in palveluita.

Eri liikennevirrat, toisin sanoen protokollayhteydet, voidaan helpommin eristää toisistaan kun jokaiselle luodaan oma IPSec SA. Liikennevirtojen yhdistäminen voi tapauksessa, jos- sa käytetään salausta ilman eheystarkistusta, mahdollistaa toisen virran selvätekstin ohjaa- misen toisen virran käyttäjälle. Tämän haavoittuvuuden esitti Steve Bellovin IETF:n konfe- renssissa huhtikuussa 1995. Tosin, yleisesti ei ole löydetty yhtään syytä, miksi salausta pi- täisi käyttää ilman eheyden suojaamista, joten tämä hyökkäys on hyvin epätodennäköinen. Liikennevirtojen eristäminen omiin turvallisuusassosiaatiohinsa taas voi jossain tapauksissa helpottaa liikenneanalyysia, koska eri virrat voidaan erottaa SPI:n perusteella.

Yksi puolustus kahdelle vaiheelle on tarve luoda eri tavalla suojatut turvallisuusassosiaatiot

eri liikennevirroille. Vasta-argumentti tälle on se, että miksi ei voida käyttää kaikille liikennevirroille vahvinta suojausta. Jos yksi virta suojataan tehokkaasti, eikö kannattaisi suojata myös muut yhtä tehokkaasti vaikka ne eivät niin kriittisiä olisikaan. Tosin, tästä voi seurata tehokkuusongelmia sen lisäksi, että eräissä harvinaisissa tapauksissa lainsäädäntö voi kieltää tietyltä liikenteeltä salauksen, jolloin eheysuojauksesta on silti hyötyä.

Edellisen kaltainen syy voisi olla myös tarve luoda eri SA:t eri liikenneluokille. Pakettien sekvenssinumeroita (uudelleenlähetyskykyä estämiseksi) tarkistettaessa seuraa ongelmia, jos osa turvallisuusassosiaation paketeista saapuu muita huomattavasti hitaammin perille. Tämä voi olla ongelma tulevaisuudessa, mutta nykyisessä Internetissä liikenteen luokittelu eri palveluluokkiin on erittäin harvinaista.

Salausavaimelle annetaan yleensä elinikä perustuen sillä salatun liikenteen määrään tai avaimen ikään. Erittäin nopeissa verkoissa tämä liikenteen määrään perustuva elinikä on suhteellisen lyhyt ja salausavaimen vaihto alkaa olla säännöllinen toimenpide. Toiminta on yksinkertaisempaa, jos liikenteen osapuolilla on käytössään ensimmäisen vaiheen turvallisuusassosiaatio, jonka suojassa voidaan sopia uusi avain sen sijaan, että pitää ensin luoda uusi turvallisuusassosiaatio ja tämän käyttöön siirtymisen jälkeen tuhota vanha.

Mielestäni paras argumentti kahden erillisen vaiheen puolesta on sen mahdollistama suojattu merkinantokanava. Edellä mainitun salausavaimen vaihdon lisäksi sitä voidaan käyttää välittämään tietoa virhetilanteista, osapuolten tukemista ominaisuuksista sekä tarkistamaan toisen osapuolen hereilläolo. Kaikki nämä ominaisuudet parantavat protokollan vakautta ja mahdollisuutta toipua virhetilanteista oikein, koska merkinantoviesteihin voidaan luottaa.

IKEv2:n suunnittelussa ei ole haluttu muuttaa konseptia aivan kokonaan. Osaksi siitä syystä, että järjestelmien muuttaminen uutta protokollaa tukevaksi olisi helpompaa, osaksi siksi että sillä on omat kiistattomat etunsa. Mekanismi, jossa ensimmäisen vaiheen neuvottelun tuloksena on luotu sekä IKE SA että IPsec SA, näyttää parhaimmalta mahdolliselta ratkaisulta. Tällä tavalla ensimmäinen käytettävä turvallisuusassosiaatio saadaan luoduksi mahdollisimman nopeasti, säilyttäen silti kaikki kaksivaiheisuuden edut. IKEv2:n määrittelemät uudet ominaisuudet kuten NAT-yhteensopivuus ja mahdollisuus pyytää IP-osoite on myös helpompaa toteuttaa suojatun yhteyden päälle. Menetelmä skaalautuu hyvin erilaisiin ympäristöihin: kevyessä kokoonpanossa ei ole välttämätöntä toteuttaa erillistä lapsi-SA:iden

neuvottelua, mutta suurien käyttäjämäärien tietoturvareitittimille se on erittäin hyvä ominaisuus.

JFK:n suunnittelijat ovat tehneet erittäin pelkistetyn protokollan, joka neuvottelee turvallisuusassosiaatiot yhdessä vaiheessa. Sillä on omat etunsa tilanteessa, jossa liikennemäärät ovat pienet ja turvallisuusassosiaatioita luodaan harvoin. Sen skaalautuvuus on kuitenkin huono, eli tietoturvareitittimien väliseen, mahdollisesti useampien tuhansien, turvallisuusassosiaatioiden luomiseen se on liian raskas.

### 7.1.2 Algoritmien neuvottelu

Liikenteen suojaamisessa käytettävien algoritmien neuvottelu etenee kaikissa tässä työssä tarkasteltavissa avaintenvaihtoprotokollissa siten, että yhteyden aloittaja kertoo ne algoritmien yhdistelmät, joita tukee ja jotka kokee sopiviksi juuri tähän yhteyteen. Vastaaja valitsee näiden joukosta yhden yhdistelmän samoin kriteerein ja kertoo tämän yhteyden aloittajalle. Jos vastaaja ei kelpuuta mitään ehdotetuista yhdistelmistä, on aloittajan ehdotettava muita algoritmeja tai hyväksyttävä se, että yhteyttä ei voida muodostaa.

IKE mahdollistaa erittäin monipuolisen ja tarkan algoritmien neuvottelun aliluvussa 4.1.6 kerrotulla tavalla. Jokainen algoritmien yhdistelmä tarvitsee oman ehdotuskuormakenttensä, esimerkiksi: 3DES-CBC salaukseen, HMAC-MD5 eheyden tarkistamiseen ja Diffie-Hellman -ryhmä numero kaksi avaimen luomiseen. Jos haluttaisiin ehdottaa edellisen esimerkin mukainen yhdistelmä myös HMAC-SHA1 -algoritmilla MD5:n sijasta, tarvittaisiin taas uusi ehdotuskuormakenttä. Vaikka tämän kaltaisella neuvottelulla kieltämättä saadaan muodostumaan juuri haluttu algoritmien yhdistelmä, on sillä myös haittapuolia. Ehdotuskuormakenttien määrä kasvaa erittäin voimakkaasti implementaation tukemien algoritmien funktiona. Esimerkiksi uusi salausalgoritmi, olettaen sitä haluttavan käyttää kaikkien MAC-algoritmien kanssa, usein tuplaa tarvittavien kuormakenttien määrän.

Yksi JFK:n suunnitteluperiaatteista – neuvottelemattomuus – kertoo sen lähestymistavan algoritmien neuvotteluun. Vastaaja ilmoittaa *GRPINFO*-kentässä tukemansa algoritmit. Neuvottelua ei voida jatkaa, jos aloittaja ei tue tai halua käyttää näitä algoritmeja. Tämä ajattelutapa perustuu oletukseen, että yhteyden osapuolet ovat toisilleen tuttuja, jolloin toisen osapuolen käyttämät suojausmenetelmätkin ovat ennestään tuttuja. Jos osapuolet taas

ovat vieraita, on vastaajalla oikeus valita haluamansa suojaustaso.

IKEv2:n neuvottelumekanismi on vaihtunut useaan kertaan sen määrittelytyön aikana. Tämän diplomityön alkuperäisenä lähdeviitteenä olleessa draftin toisessa versiossa oli valmiiksi määritellyt vaihtoehdot. Seuraaviin versioihin se muutettiin vastaamaan IKE:n neuvottelua hieman yksinkertaistettuna, niin sanottu ”a la carte”. Tämän hetken drafti taas määrittelee numeroidut valmiiksi määritellyt vaihtoehdot, mikä mielestäni on paras vaihtoehto. Se yksinkertaistaa kuormakenttien parsimista sekä antaa IETF:lle mahdollisuuden karsia pois turvattomat algoritmien yhdistelmät. IETF voi määrittellä neuvottelunumeron vain sellaisille algoritmien yhdistelmille, jotka se on todennut turvallisiksi. Niin sanotun ”suites”-menetelmän avulla voidaan myös vähentää suhteellisen tarpeettomiksi osoittautuneiden kuljetus-moodin ja AH-protokollan käyttöä, määrittelemällä niille vain hyvin vähän neuvottelunumeroita.

Ennen tämän diplomityön valmistumista on taas ilmennyt halukkuutta vaihtaa IKEv2:en neuvottelu ”a la carte” -tyyliseksi, mikä ilmentää kahden menetelmän välisen valinnan tekemisen vaikeutta.

### 7.1.3 Monimutkaisuus

Protokollan suunnittelu on aina kompromissi monimutkaisuuden ja monipuolisuuden sekä yksinkertaisuuden ja implementoinnin helppouden välillä. IKE on suunniteltu monipuolisuuden ehdoilla ja se onkin kärsinyt siitä huomattavasti. Se on paisunut niin isoksi, että kokonaisuutta on enää vaikea hahmottaa. Tämän vastapainoksi suunniteltu JFK on mennyt toiseen äärimmäisyyteen ja se on suunniteltu niin yksinkertaiseksi kuin avaintenvaihtoprotokolla on mahdollista suunnitella. Sen ominaisuudet ovat niin rajoittuneet, että se haittaisi esimerkiksi tulevaisuudessa uusien salausalgoritmien käyttöönottoa. Näiden välimaastoon sijoittuva IKEv2:n suunnittelussa on mielestäni onnistuttu tekemään hyvä kompromissi tekemättä protokollasta kuitenkaan liian raskasta. Sen ominaisuudet ovat riittävät: Ne käsittävät muun muassa uusia, tarpeelliseksi katsottuja, NAT-yhteensopivuuteen liittyviä toimintoja. Määrittelydokumentti on helposti luettavaa ja siitä on mahdollista hahmottaa miten protokolla kokonaisuutena toimii.

## 7.2 Avainten jakelumenetelmät

Maailmanlaajuista PKI-järjestelmää on odotettu pitkään. Monet hyvin hyödylliset protokollat tarvitsisivat toimivan sertifikaattien infrastruktuurin, jotta ne saisivat tarvitsemansa salaus- ja autentikointiavaimet. Näihin protokoliin kuuluva IPSec on kuitenkin kehittänyt itselleen riittävän mekanismin, jolla tarvittavat sertifikaatit voidaan siirtää. Tämän on mahdollistanut IPSec-protokollan reaaliaikaisuus: Koska protokollan molemmat osapuolet ovat aktiivisia samanaikaisesti, voidaan sertifikaatit lähettää osana turvallisuusassosiaation neuvottelua. Tämä ei ole mahdollista esimerkiksi sähköpostin lähettäjän autentikoinnissa johdun sähköpostijärjestelmän toimintamekanismista.

Tässä alaluvussa tarkastellaan kolmen käytössä olevan julkisten avainten jakelumenetelmän tärkeimpiä ominaisuuksia sekä selvitetään mihin toimintaympäristöön ne parhaiten sopivat. Menetelmät ovat certificate payload, opportunistic encryption ja LDAP.

### 7.2.1 Yleiset ominaisuudet

Yksi tapa vertailla avainten jakelumenetelmien ominaisuuksia, on jakaa ne neljään osaluokeseen seuraavasti: paikasta riippumattomuus, suorituskyky ja saatavuus, anonymi vai autentikoitu yhteys ja yhteensopivuus. [15, s. 126] Ominaisuuksista suorituskyky ja saatavuus käsitellään seuraavassa aliluvussa ja muut tässä aliluvussa.

Riippumattomuus paikasta tarkoittaa järjestelmän ominaisuutta noutaa haluttu tieto asiakkaalle ilman, että asiakkaan tarvitsee tietää mistä tieto on haettu. Klassinen esimerkki tällaisesta järjestelmästä on nimipalvelu, jossa asiakas voi aina ottaa yhteyden omaan nimipalvelimeensa ja luottaa siihen, että tämä selvittävää halutun tieton ottamalla yhteyden muihin nimipalvelimiin. Tässä työssä testatuista menetelmistä LDAP ja OE tarjoavat nämä ominaisuudet. LDAP-palvelimet voivat CIP-protokollan (Common Indexing Protocol) avulla hakea tietoa toisiltaan pyynnön ketjutus -nimisellä mekanismilla. OE, nimipalvelun varaan rakennettuna, luonnollisesti tarjoaa asiakkaille paikasta riippumattomuuden. Certificate payload -menetelmä (CP) perustuu siihen, että jokaisella osapuolella on itsensä autentikointiin tarvittavat sertifikaatit, jotka se voi tarvittaessa lähettää vastapuolelle. Jos sertifikaatteja jostain syystä ei ole saatavilla, tai ne ovat vanhentuneet, ei CP-menetelmässä ole mitään keinoa

viitata paikkaan, josta ne olisivat saatavilla.

LDAP-palvelu mahdollistaa sekä autentikoidut että anonyymit yhteydet. Anonyymi yhteys tulee kyseeseen yleisen palvelun yhteydessä. Tällainen voisi olla vaikkapa väestörekisterikeskuksen Suomen kansalaisille tarjoama sertifiikaattihakemisto. Yrityksen sisäiseen tai yritysten väliseen kommunikointiin tarkoitettut sertifiikaatit taas on hyvä sijoittaa hakemistoon, johon vaaditaan autentikointi. OE ei tarjoa mitään keinoa autentikoida asiakas, CP-menetelmä autentikoi sertifiikaattien vastaanottajan osana IKE SA -neuvottelua.

Yhteensopivuus on OE-menetelmän heikko kohta. Järjestelmä on FreeS/WAN-ohjelmiston tekijöiden suunnittelema ja toiminnan määrittelevä dokumentti on vasta draftin asteella. Drafti ei ole saanut juurikaan kannatusta ja tämän takia OE-menetelmää voi käyttää vain FreeS/WAN-järjestelmien välillä. Certificate payload ja LDAP sen sijaan ovat IETF:n määrittelemiä menetelmiä ja kaikki määrittelyn mukaiset toteutukset ovat keskenään yhteensopivia.

## 7.2.2 Suorituskyky ja saatavuus

Järjestelmä joutuu mahdollisesti tekemään kyselyitä erillisille ja jopa organisaation ulkopuolisille palvelimille selvittäessään IKE SA:n autentikointiin vaadittavia sertifiikaatteja. IKE SA:n neuvottelun aikana suoritettavat haut voivat pidentää huomattavasti neuvotteluun kuluvaan aikaan. Lisäksi, järjestelmän riippuvuus useammasta palvelimesta heikentää sen toimintavarmuutta. Tässä suhteessa CP-kuormakenttä on nopein ja toimintavarmin menetelmä. Kuten kuvasta 6.2 näkyy, ei IKE-neuvottelun ulkopuolisiin palvelimiin tarvitse ottaa yhteyttä. Menetelmä on siis täysin riippumaton muista palvelimista ja täten hyvin toimintavarma ja nopea.

Kuvan 6.3 mukaisesti etenevä OE-menetelmään hyödyntävä IKE-neuvottelu on hieman hitaampi johtuen muutamista ylimääräistä nimipalvelukyselyistä. Nimipalvelun toiminta on kuitenkin yleensä optimoitu mahdollisimman nopeaksi sijoittamalla palvelimet verkkoon lähelle asiakkaita. Tämä yhdessä nopean UDP-pohjaisen protokollan ja nimipalvelun toimintavarmuuden kanssa tekee OE-menetelmästä kohtuullisen nopean ja varman.

LDAP kulkee TCP-protokollan päällä ja siitä syystä kärsii raskaasta kolmitiekättelystä ja

yhteyden sulkemisesta. LDAP-palvelimia ei myöskään usein monisteta samassa mittakaavassa kuin nimipalvelimia, joten palvelin voi olla verkon topologiassa hyvinkin kaukana asiakkaasta. Testiverkon tapauksessa, vaikka palvelin oli samassa aliverkossa tietoturvareitittimen kanssa, oli IKE-neuvottelun loppuun saattamiseen kulunut aika selvästi muita menetelmiä pidempi. Käytännön realistisessa verkossa ero voi olla vielä suurempi ja tällöin yhteyden muodostamiseen kulunut aika voi muodostua liian pitkäksi.

### 7.2.3 Skaalautuvuus

Järjestelmässä olevien asiakkaiden määrän kasvaessa skaalautuvuus muodostuu olennaiseksi ominaisuudeksi. Muutaman käyttäjän järjestelmässä asiakkaiden ja palvelimien konfiguraatiot ja sertifikaatit voi asettaa käsin, mutta komponenttien määrän kasvaessa satoihin tai tuhansiin on keskitetty hallinta ja järjestelmän sujuva toiminta ensiarvoisen tärkeää. Sujuvan toiminnan kannalta on myös tärkeää, että kriittiset pullonkaulaksi muodostuvat kohdat voidaan monistaa tiedon saatavuuden varmistamiseksi.

LDAP-palvelimia käyttävä järjestelmä on sekä hallinnan että verkon käytön kannalta skaalautuvien. Palvelimien välisen tiedon synkronoinnin ansiosta sertifikaatteihin liittyvät tiedot tarvitsee päivittää vain yhdelle palvelimelle, josta ne päivittyvät automaattisesti muille palvelimille. Asiakkaat eivät tarvitse muuta sertifikaatteihin liittyvää konfiguraatiota kuin käyttämänsä LDAP-palvelimen osoitteen. Palvelimen kuorman kasvaessa tilanne voidaan korjata lisäämällä verkkoon uusia palvelimia.

OE-järjestelmä on myös hyvin skaalautuva. Koska se pohjautuu DNS-järjestelmään, se ei muodosta pullonkauloja verkkotopologiaan, jos nimipalvelu on hoidettu asianmukaisesti. Konfiguroinnin tarve on keskittynyt pelkästään nimipalvelimiin asiakkaiden toimiessa täysin ilman konfiguroinnin tarvetta menetelmän dynaamisen tietoturvareitittimen selvityksen ansiosta. LDAP-menetelmän kaltaisesti yhdelle nimipalvelimelle tehdyt konfiguraatiomuutokset päivittyvät automaattisesti muille nimipalvelimille.

Käytettäessä CP-kuormakenttää, ei yhteyksiä muille kuin tietoturvareitittimille tarvitse ottaa. Järjestelmän skaalautuvuus verkon topologian kannalta on siis erittäin hyvä, koska pullonkauloja ei voi syntyä. Sertifikaattien asentaminen ja ajan tasalla pitäminen kuitenkin vaatii asiakkaiden määrään verrannollisen ajan. Tietoturvareitittimien määrän kasvaessa serti-

fikaattien ylläpito voi olla hyvinkin työlästä, riippuen sertifiikaattien voimassaoloajasta ja peruutettujen sertifiikaattien määrästä.

#### 7.2.4 Oikea ympäristö

Jokaisella esiteltyllä menetelmällä on omat hyvät ja huonot puolensa. Erilaiset käyttöympäristöt vaativat järjestelmiltä erilaisia ominaisuuksia, lisäksi käyttäjien määrä ja liikenteen suojauksen tarve – päästä päähän vai tietoturvareitittimeltä tietoturvareitittimelle – asettavat osaltaan järjestelmälle vaatimuksia.

Sertifiikaattien kuljettaminen certificate payload -kuormakentässä on luonnollinen tapa protokollassa, jossa molemmat osapuolet ovat yhtä aikaa aktiivisia. Näin sertifikaatit saadaan aina silloin, kun niitä tarvitaan, ilman että niitä pitäisi tallentaa autentikoivalle koneelle. Järjestelmän hallinnan tehottomuuden vuoksi sen paras käyttöympäristö on organisaation eri konttoreiden välisen liikenteen sekä etätyöntekijöiden ja työpaikan välisen liikenteen salaaminen, käsittäen muutamia käsin konfiguroituja VPN-yhteyksiä. Tällöin tosin sen paras ominaisuus, yhteyden muodostamisen nopeus, ei ole kovin olennainen.

LDAP soveltuu edellisen kaltaisen ympäristön lisäksi tilanteeseen, jossa käytössä on runsaasti VPN-yhteyksiä, kuten esimerkiksi osastojen välinen ja organisaatioiden välinen liikenne. Sen autentikointiominaisuudet sekä keskitetty hallinta tekevät siitä paremmin skaalautuvan laajamittaiseen käyttöön.

Opportunistic encryption -menetelmä on suunniteltu hieman edellisistä poikkeavaan ympäristöön. Sen tavoitteena on, että kaikki Internetin liikenne olisi salattua. Tämä on tarkoituksenmukainen tavoite langattomissa verkoissa ja kotikäytössä, mutta yritysmaailmassa sille on vaikea löytää perusteita. Yrityksen osastojen sisäverkon liikenteen salaaminen on usein tarpeetonta ja kuluttaa turhaan hallinta- ja tietokoneresursseja. Paras kuviteltavissa oleva ympäristö sille olisikin suuri yksityiskäyttäjien aliverkko, kuten yliopiston kampusverkko, jossa toisten käyttäjien liikenteen kuuntelu on yksinkertaista ja sitä on vaikea havaita. Järjestelmän haittapuolena on sen vaatima nimipalvelun DNSSEC-ominaisuus. Suojattu nimipalvelu on yleistynyt huomattavan hitaasti, ja se todennäköisesti on myös OE-järjestelmän yleistymisen esteenä.

Ipssec-työryhmä ei halua IPSec-järjestelmän autentikointimekanismien olevan riippuvainen muista määrittelyistä ja luottaa CP-kuormakentän täyttävän sertifikaattien siirtämiseen liittyvät tarpeet. Sähköpostilistalla käymieni keskustelujen pohjalta minulle muodostui käsitys, että työryhmä virallisesti tukee CP-menetelmää, ja valmistajat voivat halutessaan toteuttaa muita rajapintoja sertifikaattien noutamiselle. Tämä on mielestäni hyvä periaate huomioon ottaen PKI-järjestelmän hidas yleistymisen ja toimivan IPSec-järjestelmän tarve.

## 8 Yhteenveto

Julkisen avaimen kryptografia on mullistanut tietoturva-alan ja -sovellukset salaisen avaimen kryptografiaan verrattuna ylivoimaisilla ominaisuuksillaan. Kahden erillisen avaimen, julkisen ja yksityisen, käyttö on mahdollistanut monia mielenkiintoisia ja hyödyllisiä sovelluksia. Saadakseen täyden hyödyn julkisen avaimen kryptografian tarjoamista ominaisuuksista, sovellukset tarvitsevat toimivan järjestelmän toisten osapuolten julkisen avaimen noutamiseen ja sen oikeellisuudesta varmistumiseen. Tämä diplomityö vertailee kolmen, hyvin erilaisella tavalla ongelmaa lähestyneen, menetelmän ominaisuuksia sekä teoreettisesta että testaustyön tuloksena syntyneestä käytännön näkökulmasta.

IPSec-protokolla on ratkaissut sertifikaattien saatavuuden ongelman määrittelemällä keinon kuljettaa tarvittavat sertifikaatit osana protokollan viestejä. Tämä on nopea ja varmatoiminen menetelmä sopien rajoitettuun ja luonteeltaan staattiseen ympäristöön. Se myös tekee IPSec järjestelmän riippumattomaksi julkisen avaimen infrastruktuurin kehittämisen vaikeuksista.

Lightweight Directory Access Protocol (LDAP) on järeämpi ratkaisu joka sopii myös laajempaan, jopa maailmanlaajuiseen, käyttöön. Sen vahvuudet on helppo laajennettavuus ja keskitetty hallinta. Internet Engineering Task Force on myös selvästi halukas kehittämään LDAP:ia jatkossakin vastaamaan sertifikaattien jakelun esille tuomiin haasteisiin.

Opportunistic encryption on menetelmä jonka lähestymistapa ongelmaan on hyvin erilainen kuin mitä on tähän asti nähty. Sen tavoitteena on mahdollistaa salattu liikenne minkä tahansa kahden aseman välillä Internetissä. Idea nimipalvelun käyttämisestä avainten jake-

luun ei sinällään ole uusi ja käyttöönottovaiheessa voidaan saada huomattavia etuja käytettäessä valmista maailmanlaajuisia hajautettua tietokantaa. Järjestelmän heikkous kuitenkin on tarve suojatulle nimipalvelulle. DNSSEC-järjestelmän yleistymisestä voi riippua myös opportunistic encryption -menetelmän tulevaisuus.

Internet Key Exchange -protokollan seuraajan suunnittelu on vielä osittain kesken. IETF:n komiteatyöskentelynä suoritettava suunnittelu on ollut hidasta johtuen osaltaan sähköpostin välityksellä käytävästä keskustelusta, osaltaan siitä, että kaikkien listalla vaikuttavien mielipiteet ja toivomukset pitää yrittää ottaa huomioon. Protokollan kehitystyön seuraaminen alusta lähtien on ollut erittäin mielenkiintoista ja opettavaista. Kehitystyötä seuraamalla saa ymmärryksen tehtyjen päätöksiä motiiveista ja ongelmista.

Kahdesta IKE:n seuraajaksi tarkoitettua määrittelystä, JFK:sta ja IKEv2:sta, ipsec-työryhmä on valinnut jälkimmäisen jatkokehitystä varten. Useiden parannuksien ja ominaisuuksien lisäämisen jälkeen siitä on muodostumassa hyvä seuraaja monien liian monimutkaisena pitämälle IKE:lle. Tietoturvaprotokollan turvallisuuden ja käyttökelpoisuuden näkee kuitenkin vasta ajan ja kokemuksen myötä.

# Lähdeluettelo

- [1] RFC2401; S. Kent, R. Atkinson. *Security Architecture for IP*, November 1998.
- [2] N. Doraswamy , D. Harkins. *IPSec: The New Security Standard for the Internet Intranets, and virtual Private Networks*, Prentice Hall PTR, 1999.
- [3] RFC2409; D. Harkins, D. Carrel. *The Internet Key Exchange*, November 1998 .
- [4] RFC2403; C. Madson, R. Glenn. *The Use of HMAC-MD5-96 within ESP and AH*, November 1998.
- [5] RFC2404; C. Madson, R. Glenn. *The Use of HMAC-SHA-1-96 within ESP and AH*, November 1998.
- [6] RFC2406; S. Kent, R. Atkinson. *IP Encapsulating Security Payload*, November 1998.
- [7] RFC2405; C. Madson, N. Doraswamy. *The ESP DES-CBC Cipher Algorithm With Explicit IV*, November 1998.
- [8] RFC2410; R. Glenn, S. Kent. *The NULL Encryption Algorithm and Its Use With IPsec*, November 1998.
- [9] RFC2407; D. Piper. *The Internet IP Security Domain of Interpretation for ISAKMP*, November 1998. s. 1, IESG Note.
- [10] *Advanced Encryption Standard*. <http://csrc.nist.gov/encryption/aes/>, December 2001.
- [11] R. Glenn, S. Frankel, S. Kelly. *The AES Cipher Algorithms and Their Use With IPsec*. draft-ietf-ipsec-ciph-aes-cbc-04.txt, June 2002. Internet-draft, work in progress.
- [12] R. Housley *Using AES Counter Mode With IPsec ESP*. draft-ietf-ipsec-ciph-aes-ctr-00.txt, July 2002. Internet-draft, work in progress.
- [13] W. Stallings *Data & Computer Communications*, Prentice Hall PTR 2000.
- [14] RFC3280; R. Housley, W. Polk, W. Ford, D. Solo. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, April 2002.
- [15] R. Housley, T. Polk. *Planning for PKI*, Wiley 2001.
- [16] RFC2631; E. Rescorla. *Diffie-Hellman Key Agreement Method*, June 1999.
- [17] RFC2408; D. Maughan, M. Schertler, M. Schneider, J. Turner. *Internet Security Association and Key Management Protocol (ISAKMP)*, November 1998.

- [18] RFC2412; H. Orman. *The OAKLEY Key Determination Protocol*, November 1998.
- [19] H. Krawczyk. *SKEME: A Versatile Secure Key Exchange Mechanism for Internet*, <http://www.research.ibm.com/security/skeme.ps>.  
Vierailtu 10.4.2003.
- [20] FreeS/WAN Project [www.freeswan.org](http://www.freeswan.org).
- [21] C. Kaufman. *Internet Key Exchange (IKEv2) Protocol*.  
draft-ietf-ipsec-ikev2-05.txt, January 2003. Internet-draft, work in progress.
- [22] B. Aboba, William Dixon. *IPsec-NAT Compatibility Requirements*.  
draft-ietf-ipsec-nat-reqts-04.txt, March 2003.
- [23] RFC2284; L. Blunk, J. Vollbrecht. *PPP Extensible Authentication Protocol (EAP)*,  
March 1998.
- [24] W. Aiello, S.M. Bellovin, M. Blaze, R. Canetti, J. Ioannidis, A.D. Keromytis,  
O. Reingold. *Just Fast Keying (JFK)*. draft-ietf-ipsec-jfk-04.txt,  
Internet-draft, work in progress.
- [25] C. Kaufman, R. Perlman, M. Spencer *Network Security, PRIVATE Communication  
in a PUBLIC World*, Prentice Hall PTR, 2002.
- [26] M. Richardson, D. Redelmeier. *Opportunistic Encryption using The Internet Key  
Exchange (IKE)*. draft-richardson-ipsec-opportunistic-10.txt,  
July 2002. Internet-draft, work in progress.
- [27] digitoday. Jaakko Kuivalainen. *Internetin juuripalvelimet hyökkäyksen kohteena*.  
[http://www.digitoday.fi/digi98fi.nsf/pub/te20021023151734\\_kni\\_61124284](http://www.digitoday.fi/digi98fi.nsf/pub/te20021023151734_kni_61124284)  
Vierailtu 10.4.2003.
- [28] RFC2535; D. Eastlake. *Domain Name System Security Extensions*, March 1999.
- [29] International Organization for Standardization [www.iso.org](http://www.iso.org).
- [30] RFC3377; J. Hodges, R. Morgan. *Lightweight Directory Access Protocol (v3): Technical  
Specification*, September 2002.
- [31] RFC2587; S. Boeyen, T. Howes, P. Richard. *net X.509 Public Key Infrastructure  
LDAPv2 Schema*, June 1999.
- [32] ASN.1 Information Site <http://asn1.elibel.tm.fr/en/index.htm>.
- [33] GNU Zebra – routing software [www.zebra.org](http://www.zebra.org).
- [34] Debian GNU/Linux – The Universal Operating System [www.debian.org](http://www.debian.org).
- [35] Red Hat – Linux, Embedded Linux and Open Source Solutions [www.redhat.com](http://www.redhat.com).

[36] The Ethereal Network Analyzer [www.ethereal.com](http://www.ethereal.com).