

# **Dokumentation über IPSec**



**von  
Joana Schweizer  
und  
Stefan Schindler**

## Inhaltsverzeichnis

1 Einleitung.....	3
1.1 Warum Sicherheit?.....	3
1.2 Datenschutz allgemein.....	3
1.3 Datenschutz für eine Firma.....	3
1.4 Eine sichere Verschlüsselung.....	3
2 Verschlüsselungsarten.....	4
2.1 Synchrone Verschlüsselung.....	4
2.2 Asynchrone Verschlüsselung.....	4
3 Datei-Schlüssel und Zertifikate.....	4
3.1 Öffentliche Schlüssel.....	4
3.2 Zertifikate.....	5
4 IPSec.....	5
4.1 Geschichte.....	5
4.2 Funktionsweise.....	5
4.2.1IKE (Internet Key Exchange).....	6
4.2.1.1 ISAKMP.....	6
4.2.1.1.1 Phase 1.....	7
4.2.1.1.1.1 Main Moduls.....	7
4.2.1.1.2 Phase 2.....	7
4.2.1.2 Firewall.....	7
4.2.2AH (Authentication Header).....	7
4.2.2.1 Transport Mode.....	7
4.2.2.2 Tunnel Mode.....	7
4.2.2.3 Firewall.....	8
4.2.3ESP (Encapsulating Security Payload).....	9
4.2.3.1 Transport Mode.....	9
4.2.3.2 Tunnel Mode.....	9
4.2.3.3 ESP-Trailer.....	9
4.2.3.4 Firewall.....	10
5 Glossar.....	11
6 Quellen.....	13

# 1 Einleitung

## 1.1 Warum Sicherheit?

Bei der Sicherheit wollen grundsätzlich immer folgende Punkte abgedeckt werden:

- Vertraulichkeit: Andere dürfen die Daten nicht lesen können.
- Integrität: Der Inhalt darf nicht verfälscht werden.
- Authentizität: Sender & Empfänger müssen "echt" sein.

## 1.2 Datenschutz allgemein

Der Datenschutz bewahrt den Einzelnen vor dem Missbrauch seiner Daten. Der technische Fortschritt ermöglicht heutzutage eine immer schnellere und umfangreichere Erfassung persönlicher Daten. Sowohl Behörden als auch die Privatwirtschaft sammeln zahlreiche Informationen über ihre Kunden. Namens-, Adress- und Geburtsdaten werden ebenso gespeichert, wie Informationen zum Beispiel über das Kaufverhalten oder das Einkommen.

Für einen Nutzer wird es immer schwieriger zu beurteilen, wer was für Daten über ihn speichert. Ob diese Datenerfassung überhaupt erlaubt ist, können meist nur noch Spezialisten sagen.

Darum erlässt der Staat Gesetze zum Schutz der Privatsphäre. Tatsache ist, dass er im Moment stärker mit dem Aufbau verschiedener "Schnüffel"-Aktionen beschäftigt ist.

## 1.3 Datenschutz für eine Firma

Für eine Firma ist es wichtig, dass die internen Informationen auch intern bleiben. Die Integrität und die Vertraulichkeit der Daten ist besonders bei Neuentwicklungen, strategischen Informationen, Kunden- und Personaldaten. Zudem ist die Authentizität wichtig, da ein Angreifer von aussen ein grosses Interesse haben könnte die Daten zu stehlen oder zu verfälschen.

## 1.4 Eine sichere Verschlüsselung

Wenn ein Sicherheitssystem nur teilweise veröffentlicht wird, kann seine Sicherheit nicht beurteilt werden. Dadurch entsteht eine "Schein-Sicherheit", welche potentiell nicht vorhanden ist. Ein solches System könnte zum Beispiel bloss ein paar Bits vertauschen.

Die Schlüssellänge entscheidet über die Sicherheit des ganzen Systems. An diesem Punkt kann der Benutzer am meisten mitentscheiden, ob das System sicher ist.

## 2 Verschlüsselungsarten

### 2.1 Sychrone Verschlüsselung

Synchrone Verschlüsselungen sind die ältesten und einfachsten Verfahren, um Inhalte vor Fremden zu schützen. Ein bekanntes Beispiel ist die Cäsar-Verschlüsselung. Der Trick war, die Zeichen im Alphabet um eine Anzahl Stellen zu verschieben. Zum Entschlüsseln musste man nur wissen, um wie viele Stellen am Anfang verschoben worden ist.

Beim Ver- und Entschlüsseln wurde der gleiche Schlüssel verwendet. Zum Beispiel "+4". Folgende Probleme sind bereits aufgetreten:

- 1 Der Schlüssel muss immer bei allen präsent sein.
- 2 Wer den Schlüssel hat, kann die Nachrichten der Andern auch lesen.
- 3 Wird der Schlüssel geknackt,
  - 3.1 muss er zuerst allen mitgeteilt werden
  - 3.2 kann der Feind mit dem alten Schlüssel falsche Nachrichten versenden

### 2.2 Asynchrone Verschlüsselung

Die asynchrone Verschlüsselung ist komplexer als die synchrone und baut auf der erweiterten Mathematik auf. Es werden zwei Schlüssel verwendet, ein privater und ein öffentlicher.

Der öffentliche Schlüssel ist jedem bekannt. Jeder kann damit Nachrichten verschlüsseln. Die Nachrichten können mit dem öffentlichen aber nicht mehr entschlüsselt werden.

Für die Entschlüsselung braucht man den privaten Schlüssel. Dieser muss darum unter allen Umständen geheim gehalten werden, da die meisten Verschlüsselungsalgorithmen den privaten Schlüssel für die Authentifizierung verwenden und man mit dem privaten die Nachrichten lesen kann.

## 3 Datei-Schlüssel und Zertifikate

Wesentlich sicherer als Passwörter sind so genannte generierte Schlüssel. Da diese "Datei-Schlüssel" viel länger und auch zufälliger sind, können diese Verbindungen schlechte geknackt werden. Für den Verbindungsaufbau werden auf beiden Systemen verschiedene private und öffentliche Schlüssel abgelegt. Werden die Geräte gekapert hat man natürlich auch die Schlüssel. SSL und IPSec bieten ausserdem die Möglichkeit, ein Zertifikat mit einem Passwort zu sichern.

### 3.1 Öffentliche Schlüssel

Einer der grössten Vorteile der asynchronen Verschlüsselung ist der öffentliche Schlüssel. Mit ihm kann jeder eine verschlüsselte Verbindung zu einem Host aufbauen. Sollte der Host gefälscht sein, kann er mit den Daten nichts anfangen, da er den dazugehörigen

privaten Schlüssel braucht.

Auf dem Rückweg, kann nur der echte Host die Daten so verschlüsseln, dass man sie mit dem öffentlichen Schlüssel wieder entschlüsseln kann. Die Daten sind damit authentifiziert und verschlüsselt.

### **3.2 Zertifikate**

Zertifikate und öffentliche Schlüssel sind technisch gesehen das gleiche. Der Unterschied ist, dass ein Zertifikat bestätigt, also frei zugänglich bei einer öffentlichen anerkannten Stelle, ist. Der Vorteil ist, dass eine weitere Stelle sagt, dass mein Host wirklich der Host ist und nicht ein anderer sich mit einem anderen öffentlichen Schlüssel dazwischen mogeln will.

## **4 IPSec**

### **4.1 Geschichte**

IPSecurity Protocol wurde 1998 von der IETF entwickelt. Es sollte IPv4 sicherer machen und ist fester Bestandteil von IPv6. Es sollte die Authentizität, Integrität und Vertraulichkeit der Daten bei der Übertragung sicherstellen.

Von aussen muss es resistent gegen TCP-Replay-Angriffe sein.

IPSec muss intern unsichtbar arbeiten. Also bei Clientanwendungen nichts neues in die Welt stellen. IPSec arbeitet darum immer als Gateway zwischen den Netzen.

Es musste Modular sein. Das heisst, man kann die Verschlüsselungsverfahren einfach austauschen.

Dank der Modularisierung können auch die einzelnen Protokolle für die Authentifizierung oder Verschlüsselung ausgetauscht werden.

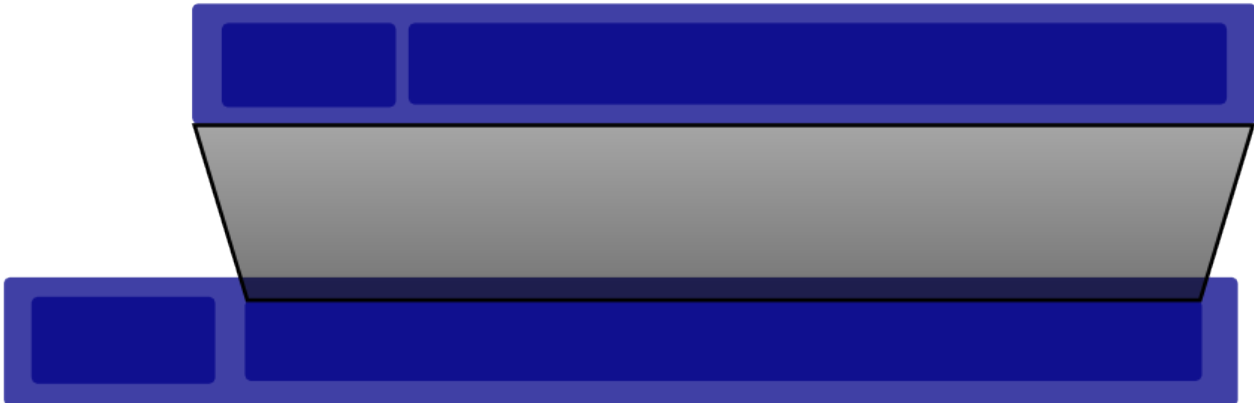
Zudem ist es Möglich, IPSec um weitere Protokolle zu ergänzen. Ein Beispiel wäre das QoS-Protokoll, welches die vorhandene Bandbreite besser verwaltet.

IPSec ist also nicht ein Protokoll, sondern eine Sammlung von Protokollen.

### **4.2 Funktionsweise**

IPSec hat zwei Modelle, den Tunnel- und den Transportmodus. Mit dem Tunnelmodus kann man ein VPN machen. Er erfordert relativ viel CPU-Leistung. Mit dem Transportmodus kann man die Kommunikation im Intranet sichern. Dies lohnt sich, wenn zwei Personal-Teams an verschiedenen Standorten sind.

In jedem Fall nutzt man die Verschachtelung im OSI-Modell auf Layer 3 & 4. Unverschlüsselt sieht dies so aus:



Am Anfang werden Header-Informationen gesendet. Danach kommt die Nutzlast, Payload. Darin wird das TCP-Paket (oben) in das IP-Paket auf Layer 3 geschrieben.

### 4.2.1 IKE (Internet Key Exchange)

In der ersten Phase des IKE wird Main Mode genutzt und eingesetzt.

Hierbei handelt derjenige, der die Verbindung aufnehmen will und derjenige der Antwortet miteinander ein SA's aus.

Der Ablauf geschieht in folgenden sechs Schritten:

1. Derjenige der die Verbindung aufbauen will sendet einen oder mehrere Vorschläge mit Authentifizierungs- und Verschlüsselungsalgorithmen.
2. Derjenige der antwortet wählt einen Vorschlag aus und bestätigt diesen.
3. Der die Verbindung aufgebaut hat sendet den öffentlichen Teil der Diffie-Hellmann-Schlüsselvereinbarung und einen zufälligen Wert.
4. Der Antwortende schickt ebenfalls den öffentlichen Teil der Diffie-Hellmann-Schlüsselvereinbarung und einen zufälligen Wert.
5. Der Initiator (derjenige der die Verbindung aufgebaut hat) berechnet die Signatur und sendet diese mit seiner Identität an den Antwortenden. Diese Daten werden mit einem symmetrischen Schlüssel verschlüsselt.
6. Der Antwortende schickt die gleichen Daten von seiner Seite an den Initiator.

Die zweite Phase die bei IKE zur Anwendung gebracht wird heisst Quick Mode. In diesem Verfahren erfolgt die gesamte Kommunikation verschlüsselt. Wie auch in der ersten Phase wird zuerst ein Vorschlag gemacht. Dieser wird zusammen mit einem Hashwert und der zufällige Wert übertragen. Danach werden die Schlüssel neu berechnet und es gehen keine Informationen aus den zuvor generierten SA's ein. Dies stellt sicher, dass niemand von den zuvor generierten Schlüsseln auf die neuen schliessen kann.

#### 4.2.1.1 ISAKMP

Das ISAKMP ist ein Protokoll das Prozeduren definiert für die Authentifikation von Kommunikationspartnern, Erstellung und Management von Security Associations, Schlüsselerzeugung sowie die Verringerung von Angriffsmöglichkeiten wie z.B die Replay-

Attacken.

#### **4.2.1.1.1 Phase 1**

Phase 1 erzeugt eine sichere Verbindung (ISAKMP-SA) über die die Sicherheitsparameter ausgehandelt werden können. Dazu werden die Parameter zur Berechnung eines Master-Keys mittels des Diffie/Hellmann-Algorithmus ausgetauscht und die Gegenstellen authentisiert.

##### **4.2.1.1.1.1 Main Moduls**

Erzeugt ISAKMP-SA. Dies ist der vorgesehene Weg.

#### **4.2.1.1.2 Phase 2**

Phase 2 definiert dann die für IPSec verwendbaren SA's zur Übertragung der Nutzdaten. Diese Phase kann sich auch während der Verbindung wiederholen.

#### **4.2.1.2 Firewall**

Das IKE läuft auf dem UDP-Port 500.

## **4.2.2 AH (Authentication Header)**

Der AH soll die Authentizität und die Integrität der übertragenen Pakete sicherstellen und den Sender authentifizieren.

AH bildet mit MD5 oder SHA-1 eine Prüfsumme des Payloads und des Headers.

#### **4.2.2.1 Transport Mode**

Da in einigen Teilen des IP-Headers die Daten auf dem Weg verändert werden müssen, können nicht alle Daten geschützt werden. Würden alle Teile des Headers geschützt werden, dürfte zwischen den beiden Gateways kein Router, da dieser den TTL Wert verändern würde, oder Switch, da dieser die MAC-Adresse verändern würde, sein. Ausserdem ausgenommen sind ausserdem TOS (Type of Service), Header-Checksummen und einige andere Felder.

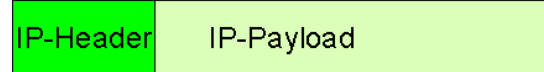
#### **4.2.2.2 Tunnel Mode**

Im Tunnel-Mode wird das ganze IP-Frame nach hinten verschoben. Davor wird ein neuer IP-Header geschrieben. Gefolgt von den Checksummen ist dann das ganze Original-Paket gegen Veränderungen gesichert.

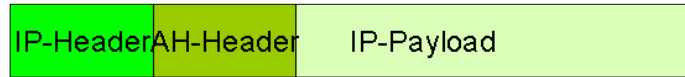


## ■ Authentication Header

Datenpaket

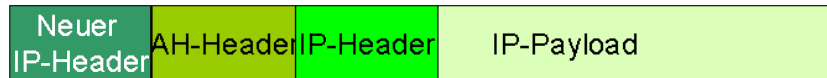


AH-Transport-Modus



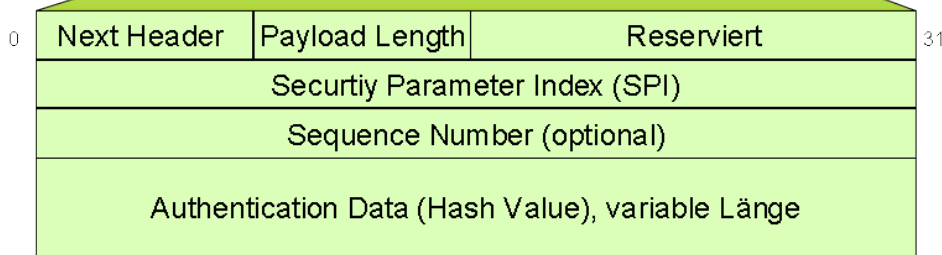
← authentisiert →

AH-Tunnel-Modus



← authentisiert →

## ■ Authentication Header Format



© Dipl. Inform. Klaus Eppeler, Heinrich-Weitz-Str. 31, 76228 Karlsruhe, Tel. 0721 / 9474621, Fax. 0721 / 9474622, E-Mail: eppeler@improve-mtc.de, www.improve-mtc.de

Next Header:	Identifiziert den Typ des Payloads, also ob es sich zum Beispiel um ein TCP (Nr. 6) oder um ein UDP (Nr. 17) handelt.
Payload Length:	Länge des AH-Headers.
Reserved:	Für zukünftige Anwendungen reserviert.
Security Parameter Index SPI:	Dieser Wert ist ein Pointer, welcher auf die Security Association SA zeigt, welche für dieses Datenpaket zuständig ist.
Sequence Number:	Schutz gegen Reply-Angriffe.
Authentication Data:	Hashwert, je nach dem welcher Hashalgorithmus verwendet wurde ist dieser Eintrag verschieden lang.

### 4.2.2.3 Firewall

Auf der Firewall wird beim Host der Port 51 verwendet.

### 4.2.3 ESP (Encapsulating Security Payload)

Das ESP-Protokoll wird verwendet, wenn der Inhalt auch verschlüsselt werden soll. ESP verwendet normalerweise eine asynchrone Verschlüsselung, wodurch der Host automatisch authentifiziert ist.

#### 4.2.3.1 Transport Mode

Im Transportmodus verschlüsselt ESP den Payload von IP, also auf Layer 3. Dazu werden ein Trailer- und ein Auth-Block angehängt. Die IP-Header Informationen sind frei zugänglich.

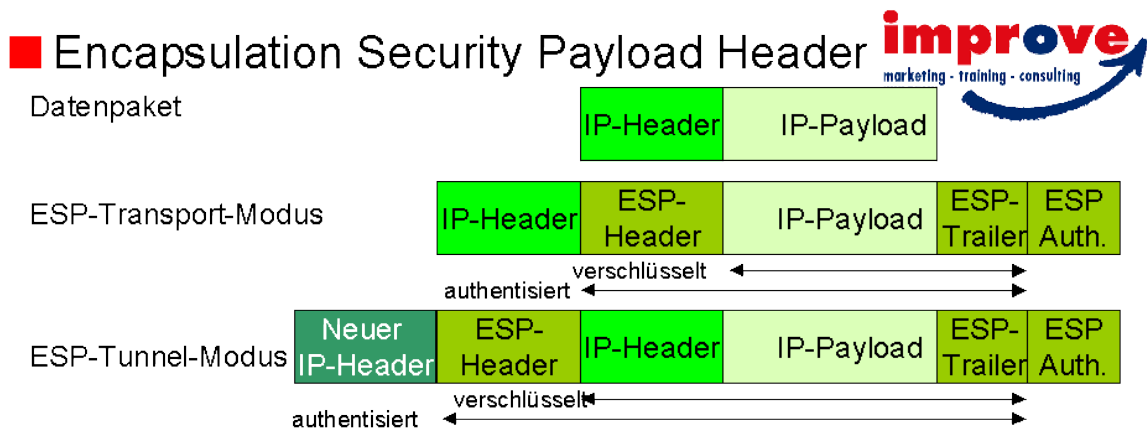
#### 4.2.3.2 Tunnel Mode

Im Tunnelmodus wird das ganze IP-Frame verpackt und verschlüsselt. Das Verschlüsselte wird dann von einem neuen Paket aufgenommen und weiter geschickt.

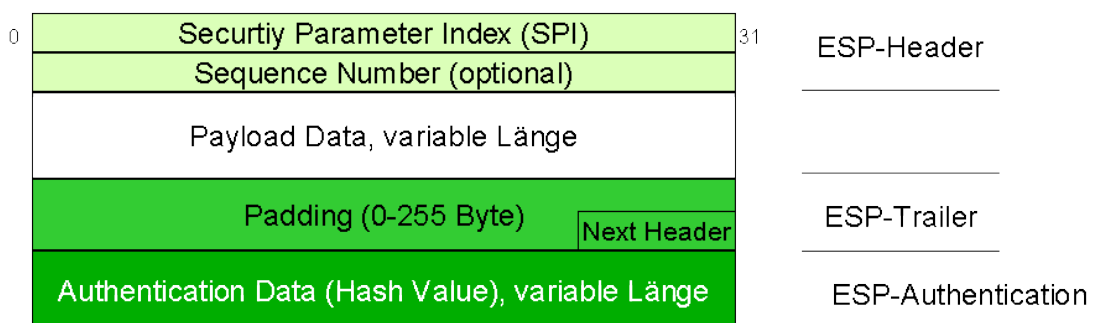
#### 4.2.3.3 ESP-Trailer

Der Trailer ist ein Block von variabler Größe. Er muss das neue IP-Paket auffüllen. Beim Auffüllen, werden zwar Daten verschwendet, von der Sicherheit her betrachtet erschwert der Vorgang aber die Entschlüsselung stark. Zudem können auch reine Trailer-Pakete geschickt werden um das transferierte Datenvolumen zu verschleiern.

Ein ESP-Paket sieht folgendermassen aus:



### ESP Header und Trailer Format



© Dipl. Inform. Klaus Eppeler, Heinrich-Weitz-Str. 31, 76228 Karlsruhe, Tel. 0721 / 9474621, Fax: 0721 / 9474622, E-Mail: eppeler@improve-mtc.de, www.improve-mtc.de

Security Parameter Index SPI:	Dieser Wert ist ein Pointer, welcher auf die Security Association SA zeigt, welche für dieses Datenpaket zuständig ist.
Sequence Number:	Schutz gegen Reply-Angriffe.
Payload Data:	Verschlüsselte Nutzdaten
Padding:	Je nach verwendetem Verschlüsselungsalgorithmus wird als Input eine ganz bestimmte Länge des Datenpakets verlangt um die Verschlüsselung durchzuführen. Das Padding dient zum Erreichen der gewünschten Länge.
Pad Length:	Länge des vorangehenden Padding Feldes.
Next Header:	Daten-Typ der Nutzdaten (TCP/UDP etc.)
Authentication Data:	Im ESP ist das Erzeugen eines Hashwertes optional, aber aus Sicherheitsgründen wird es in der Regel gemacht. Auch wenn die Daten verschlüsselt sind, wäre die Möglichkeit gegeben eine Fälschung der Daten vorzunehmen. Durch den Hashwert wird das ganz klar verunmöglicht.

#### 4.2.3.4 Firewall

ESP läuft auf dem Port 50

## 5 Glossar

<b>Begriff:</b>	<b>Erklärung:</b>
SPI (Security Parameters Index)	identifiziert in Verbindung mit der IP-Adresse und dem Sicherheitsprotokoll die Sicherheitsassoziation.
IETF (Internet Engineering Task Force)	Eine Organisation, die sich mit der technischen Weiterentwicklung des Internets befasst.
VPN (Virtual Private Network)	Ein reines Softwareprodukt (daher „virtuell“ und dient der Einbindung von entfernten Geräten eines benachbarten Netzes an das eigene (private) Netz, ohne das die Netzwerke zueinander kompatibel sein müssen.
IPv6	Internet Protokoll – Standard neben Ipv4 für die Netzschicht des OSI-Modells und regelt die Adressierung und das Routing von Datenpaketen durch ein Netz.
RFCs (Reauests for Comments)	Eine Reihe von technischen und organisatorischen Dokumenten.
TTL (time-to-live)	der Name eines Header-Feldes des Internetprotokolls, das verhindert, dass unzustellbare Pakete endlos lange von Router zu Router weiterleitet werden. Das TTL-Feld umfasst das Oktett, kann also Zahlenwerte bis max. 255 beinhalten.
TCP-Replay-Angriffe	Hierbei handelt es sich um einen Angreifer der zuvor aufgezeichnete Daten, um etwa eine fremde Identität vorzutäuschen.
Hash-Wert	Die Hash-Werte bzw. Streuwerte sind meist skalare Werte aus einer Teilmenge der natürlichen Werte. Der Hash-Wert ist eine nahezu eindeutige Kennzeichnung einer übergeordneten Menge.
MD5 (Message Digest 5)	Verbreitete Methode zur Erstellung von Hash-Werten. MD5 ist eine weit verbreitete kryptographische Hash-Funktion, welche einen 32-Byte-Hashwert erzeugt.
SHA-1 (Secure Hashing Algorithmus)	Bezeichnet eine Gruppe standardisierter kryptographische Hash-Funktion. Diese dienen zur Berechnung eines eindeutigen

	Prüfwerts für beliebige elektronische Daten.
SA (Security Associations)	Das ist ein 'Vertrag' über Sicherheitsparameter einer Kommunikationsbeziehung wie Verschlüsselungsverfahren, Authentifizierungsverfahren, Schlüsselmaterial, Gültigkeitsdauer des Schlüsselmaterials usw. Anhand dieser SA's werden dann die gesendeten Datenpaket verschlüsselt.
SSL (Secure Socket Layer)	Sitzungsbasierte Verschlüsselung auf dem OSI-Layer 5.
QoS (Quality of Service)	Beschreibt die Güte eines Kommunikationsdienstes aus der Sicht der Anwender, das heisst, wie stark die Güte des Dienstes mit deren Anforderungen übereinstimmt.
Symmetrischer Schlüssel	Bei der Ver- und Entschlüsselung wird der gleiche Schlüssel verwendet.
Asymmetrischer Schlüssel	Beim Ver- und Entschlüsseln werden unterschiedliche, nicht von einander ableitbare, Schlüssel verwendet.

## 6 Quellen

<b>Quelle</b>	<b>Adresse</b>
Wikipedia	<a href="http://de.wikipedia.org/wiki/IPsec">http://de.wikipedia.org/wiki/IPsec</a>
OpenSWAN	<a href="http://openswan.org">http://openswan.org</a>
Improve MTC	<a href="http://www.improve-mtc.de/Veroffentlichungen/VPN-DC/vpn-dc.html">http://www.improve-mtc.de/Veroffentlichungen/VPN-DC/vpn-dc.html</a>
Herrn Furrer's Buch	Lehererpult
Modulbuch 129	Buchhandlung