Virtuelle Private Netze (VPN)

Geschrieben von ~Creepy~Mind~

Version 1.3 ;-)

(Wybe Dijkstra: "Tue nur, was nur Du tun kannst.")

Copyright und Motivation und sowas

Naja was soll ich hierzu groß schreiben...

1. Wer Rechtschreibfehler findet kann sie behalten
2. Für ***KONSTRUKTIVE*** Kritik bin ich offen
3. Copyright gibs an sich natürlich nicht, ich möchte nur darum meine Mühe zu respektieren
4. ***Kopieren erwünscht !!!***
5. Geschrieben hab ich dieses Dokument, um interessierten Leuten dieses komplexe Thema zumindest ein klein wenig näher zu bringen
6. Vorkenntnisse: man sollte schonmal ein PC bedient bzw. sich ein kleinwenig mit der Netzwerktechnik beschäftigt haben

Inhalt

1. **Was ist ein VPN? (kurze Definition)**
2. **VPN Architekturen bzw. Anwendungen**
3. **Implementierungen / Protokolle / Anforderungen**
   - **3.1** ***Das Tunnelverfahren (Tunneling)***
   - **3.2** ***Vorstellung verschiedener VPN Protokolle***
     - ***3.2.1.PPTP***
     - ***3.2.2.L2TP***
     - ***3.2.3.IPSec***
       - ***3.2.3.1.Tunnel- und Transportmodus***
       - ***3.2.3.2.SA, IKE, Zertifikate***

< Anhang >

A. Main Mode
B. Aggressive Mode

1. Was ist ein VPN?

Die folgende Definition bietet einen kurzen Überblick über ein sehr komplexes Thema im EDV-Bereich, welches im weiteren Verlauf noch konkretisiert wird.

„Ein virtuelles privates Netz (VPN) ist ein Netz von logischen Verbindungen zur Übermittlung von privaten Daten/Informationen bzw. Datenverkehr.

Eine logische Verbindung ist eine Netzverbindung zwischen einem Sender und einem Empfänger, bei der der Weg der Information und die Bandbreite dynamisch zugewiesen werden.“

(Quelle: „VPN - Virtual Private Networks“ von W. Böhmer, Hanser Verlag (Juni 2005))

Die Verbindung der Netze erfolgt über einen verschlüsselten oder auch ungesicherten („Klartextübertragung“) Tunnel zwischen dem VPN-Gateway bzw. VPN-Server und dem VPN-Client.

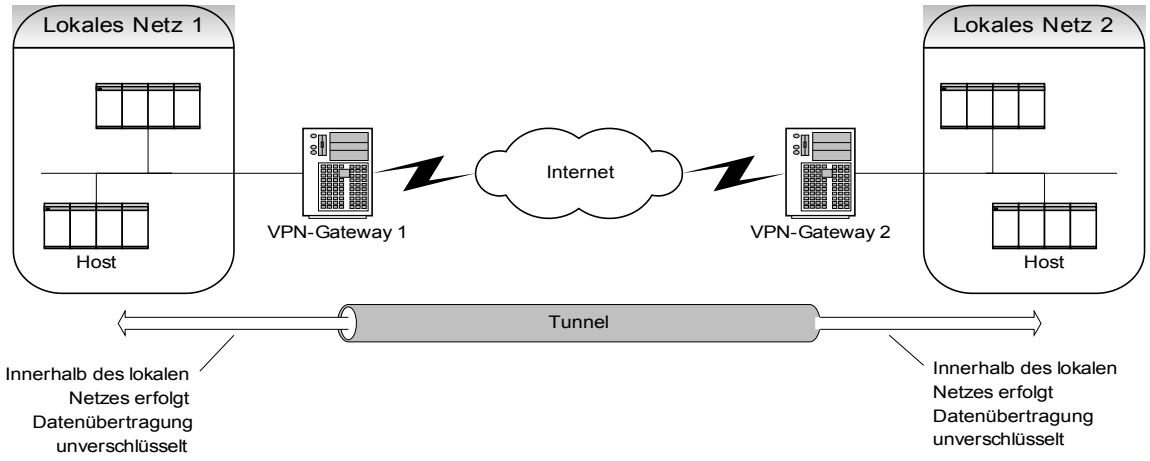
2. VPN Architekturen bzw. Anwendungen

Es haben sich im Laufe der Zeit diverse Anwendungsmöglichkeiten im Bereich der VPN herauskristallisiert, die im Folgenden näher erläutert werden.

- **Site-to-Site VPN**

Das Site-to-Site VPN ist eine Verbindung zweier lokaler Netze durch VPN-Gateways.

Dies ist die einfachste und am meisten verbreitete Form der VPN
Bei einem Site-to-Site VPN tauschen zwei lokale Netze mit ihren Stationen Daten über ein öffentliches Netz aus (z.B. das Internet). Die Kommunikation zwischen den beiden VPN-Gateways erfolgt verschlüsselt über einen Tunnel (siehe Abb.1).
Innerhalb der einzelnen lokalen Netze werden die Daten allerdings unverschlüsselt übertragen.
Der entscheidende Vorteil dieser Lösung liegt in der Tatsache, dass keine der lokalen Arbeitsstationen mit einer speziellen VPN-Software ausgestattet werden muss.
Die Gateways übernehmen in diesem Fall die gesamte Gewährleistung der Sicherheit, weshalb das VPN für die im lokalen Netz befindlichen Rechner vollkommen transparent ist.



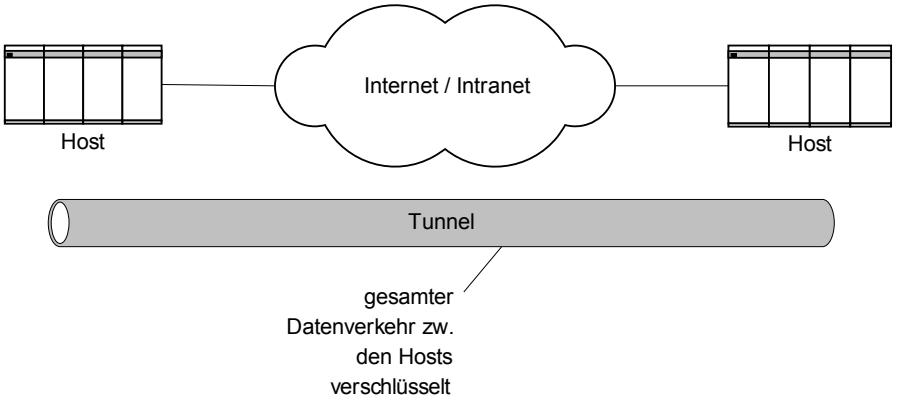
(Abb. 1: Site-to-Site VPN)

2. VPN Architekturen bzw. Anwendungen

- **End-to-End VPN**

Die End-to-End Architektur stellt eine direkte Verbindung zwischen zwei Hosts dar.

Die End-to-End Architektur ist die sicherste Lösung für eine VPN-Verbindung, da der Tunnel mit den verschlüsselten Daten die gesamte Verbindung bis zu den Hosts abdeckt (siehe Abb. 2). Damit wäre ein Angriff auf den Verbindungsweg nur schwer durchzuführen und damit fast ausgeschlossen.
Der Nachteil dieser Lösung ergibt sich aus der Tatsache, dass jeder der beteiligten Hosts eine spezielle VPN-Software benötigt und weiterhin leistungsstark genug sein sollte damit Verzögerungen der Verbindung minimiert werden können.



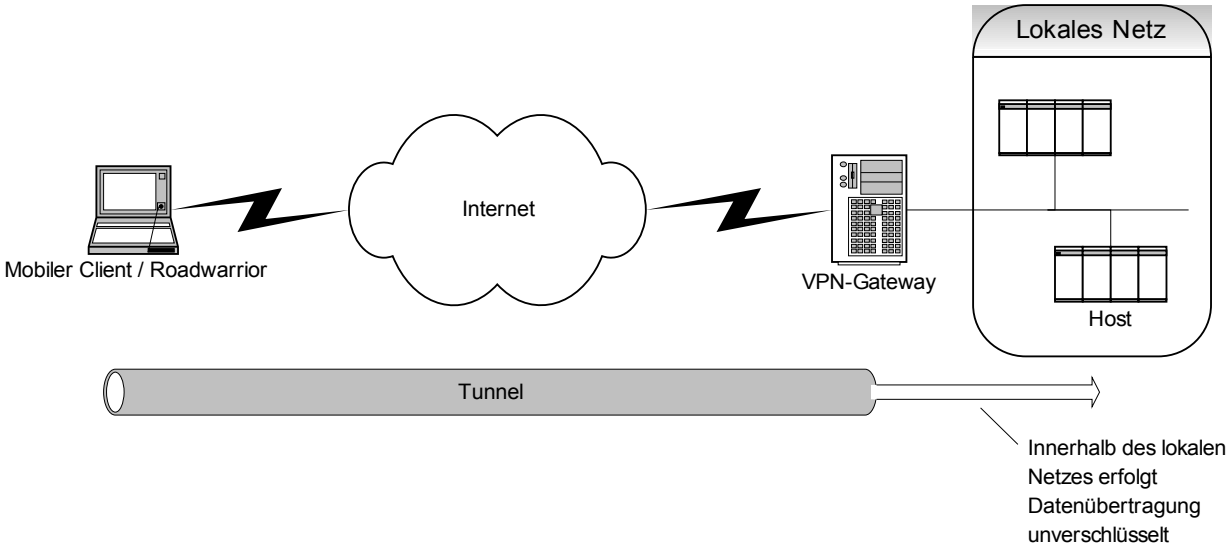
(Abb. 2: End-to-End VPN)

2. VPN Architekturen bzw. Anwendungen

- **Remote-Access VPN (End-to-Site)**

  Diese Möglichkeit ist eine Kombination aus den beiden vorangegangen VPN-Lösungen.

  Remote-Access VPNs ermöglichen einen Remotezugriff auf die Ressourcen eines Unternehmens unter Wahrung der Datensicherheit, d.h. es wird eine verschlüsselte Verbindung vom Client zum Firmennetzwerk aufgebaut (siehe Abb 3).
  Der Client wählt sich zuerst bei seinem Provider ein und baut dann automatisch einen verschlüsselten Tunnel zum VPN-Gateway auf.
  Alle Clients müssen mit einer speziellen Client-VPN-Software ausgestattet werden.
  Eine klassische Anwendung stellt die Anbindung von Außendienstmitarbeitern dar (in diesem Falle wird der Client als Roadwarrior bezeichnet).



(Abb. 3: End-to-Site VPN)

3. Implementierungen / Protokolle / Anforderungen

Grundlegende Anforderungen, die an eine VPN-Lösung gestellt werden, sind:

1. die Sicherstellung der Sicherheit und Integrität der zu übertragenden Daten

2. Benutzerauthentifizierung *(Dies beinhaltet die Überprüfung der Identität des Benutzers sowie dessen Zugriffsaktivität auf Ressourcen, welche mittels Überwachungs- und Kontoführungseinträgen überprüft wird.)*

3. Adressverwaltung (*Adressen der Clients müssen auf dem privaten Netz zugeordnet und deren Integrität sichergestellt werden)*

4. Datenverschlüsselung (D*ie über öffentliche Netze übertragenen Daten müssen vor unautorisierten Zugriffen geschützt sein)*

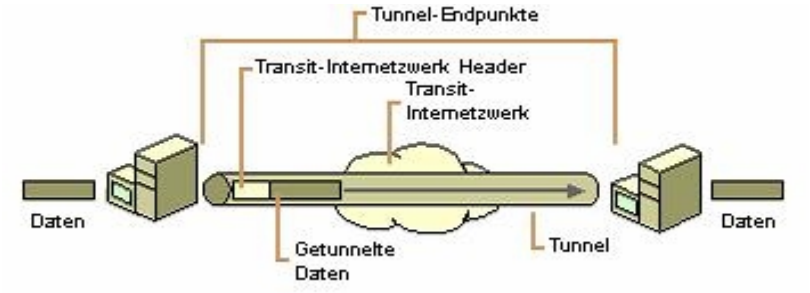
5. Schlüssel- und Zertifikatmanagement (F*ür die jeweiligen VPN-Endpunkte müssen Schlüssel (kryptische Reihenfolge aus Buchstaben, Zeichen und Zahlen) bzw. Zertifikate erstellt sowie regelmäßig aktualisiert und unter ihnen ausgetauscht werden)*

Alle in den folgenden Abschnitten behandelten Protokolle und Verfahren erfüllen diese Anforderungen.

3. Implementierungen / Protokolle / Anforderungen

3.1 Das Tunnelverfahren (Tunneling)

Das Tunnelverfahren (Tunneling; Abb. 4) bezeichnet die Übertragung von Daten für ein Netzwerk über ein Transitnetz (z.B. das Internet), wobei die zu übertragenden Datenpakete / -rahmen vom Tunnelprotokoll nicht in ihrer Ausgangsform, sondern gekapselt an einen neuen Header übertragen werden. Dieser enthält Routinginformationen, aufgrund derer die gekapselten Rahmen / Pakete das Transitnetz zwischen dem Ausgangsnetz und dem Zielnetz passieren können.
Der logische Pfad, den gekapselte Pakete nutzen, wird als Tunnel bezeichnet.
Am Zielpunkt angekommen, wird die Kapselung aufgehoben, sodass die entkapselten Datenrahmen / -pakete zum Zielort geleitet werden.
Das Tunneling beinhaltet den gesamten Prozess der Kapselung, Übertragung und Entkapselung der Pakete.



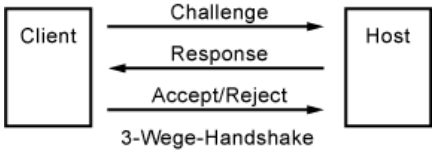
(Abb. 4: Tunnnelverfahren, Quelle: http://www.microsoft.com/)

3.2 Vorstellung verschiedener VPN Protokolle

3.2.1 PPTP

Das vorallem in Windows basierenden Netzwerken eingesetzte Point to Point Tunneling Protocol (PPTP) ist in der Sicherungsschicht des ISO/OSI-Modells implementiert und ausschließlich für den Transfer von IP, IPX und NetBEUI geeignet.
Es ermöglicht diesen Verkehr (IP, IPX u. NetBEUI) zu verschlüsseln, in einen Header zu kapseln und dann über ein privates bzw. öffentliches Netz zu senden.
PPTP nutzt PPP (Point to Point Protocol) zur Kapselung und Verschlüsselung des IP-Verkehrs.
Weiterhin dient PPTP zur gegenseitigen Authentifizierung beim Aufbau einer VPN-Verbindung und bedient sich auch hier der Möglichkeiten von PPP (in Form von CHAP und PAP).
PAP (Password Authentication Protocol) beschreibt einen 2-Wege-Handshake mit Benutzer- und Passwortabfrage. Da aber diese Daten unverschlüsselt in Klartext übertragen werden, wird stattdessen CHAP (Challenge Handshake Authentication Protocol) verwendet. Hierbei werden die Nutzerdaten verschlüsselt übertragen, vom Host abgeglichen und bei Übereinstimmung akzeptiert.
CHAP beschreibt bei der Authentifizierung einen 3-Wege-Handshake.

(Abb. 5: PAP-Authentifizierungsverfahren, Quelle: http://www.elektronik-kompendium.de/)



(Abb. 6: CHAP-Authentifizierungsverfahren, Quelle: http://www.elektronik-kompendium.de/)

3.2.2 L2TP

Das Layer-2-Tunneling Protocol (L2TP) dient dem Tunneling auf der Schicht 2 und wurde als Analogie zu PPTP entwickelt. Es vereint verschiedene Eigenschaften des PPTP und des L2F (Layer-2-Forwarding, Tunneling Protokoll und „Vorgänge“ von L2TP).
Zur Authentifizierung werden auch hier die Möglichkeiten des PPP genutzt.
Es besitzt den Vorteil, jedes Netzwerkprotokoll in den PPP-Rahmen transportieren zu können, hat aber den Nachteil, dass kein Mechanismus zum kryptischen Schutz des Tunnels beiträgt, was beispielsweise durch IPSec erfolgen kann.

3.2.3 IPSec

IPSec ist eine Erweiterung des Internet-Protocols (IP; Bestandteil von IPv6) und ein herstellerübergreifender Standard, der den Datenaustausch im Rahmen einer VPN-Lösung regelt. Alle zum IPSec-Standard gehörenden Protokolle müssen die am Anfang von Punkt 2.3 erwähnten Anforderungen erfüllen.
IPSec nutzt für den VPN-Verbindungsaufbau den Authentification-Header (AH) oder den Encapsulating Security Payload (ESP).
Die Schlüsselverwaltung innerhalb des VPN wird manuell oder durch das Internet Key Exchange Protocol (IKE) durchgeführt.

Im IPSec unterscheidet man grundsätzlich zwei Arten von Schlüsseln: Preshared Keys und Zertifikate.
Während Zertifikate als sicher gelten, können Preshared Keys eine Schwachstelle darstellen und Angreifern unter Umständen Zugang zu geschützten Daten ermöglichen. Dennoch ist die Methode des Preshared Keys weit verbreitet und stellt auch für sehr ambitionierte Cracker bzw. Hacker ein größeres Hindernis dar, vorausgesetzt der Key ist entsprechend lang und kryptisch.

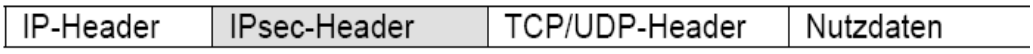
3.2.3.1 Tunnel- und Transportmodus

Der IPSec-Standard beinhaltet zwei verschiedene Modi, den Transport- und den Tunnelmodus, sowie das Authentification Header Protokoll (kurz AH; IP-Protokoll 50) und das Encapsulating Security Payload Protokoll (kurz ESP; IP-Protokoll 51).

HINWEIS: AH und ESP werden im weiteren Verlauf dieses Punktes abgehandelt

- Transportmodus

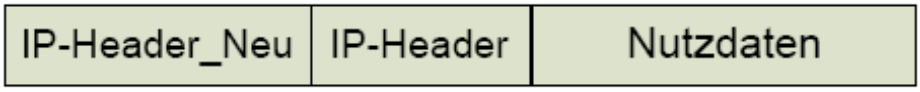
Dieser Modus findet, aufgrund seines niedrigeren Sicherheitsgrades, meist innerhalb interner Netze Anwendung sowie bei Echtzeitanwendungen.
Es wird durch Einfügen eines IPSec-Headers mit Sicherheitsinformationen nur der Inhalt des IP-Paketes geschützt und der eigentliche IP-Header verbleibt in seiner ursprünglichen Form.
Hier wird hauptsächlich mit dem zum IPSec-Standard gehöhrenden AH gearbeitet, wobei auch der Einsatz, des dem selben Standard angehörenden ESP möglich ist.



(Abb. 7: IP-Paket im Transportmodus)

- Tunnelmodus

Der Tunnelmodus findet Anwendung, wenn Verbindungen über öffentliche Netze hergestellt werden sollen. Er wird hauptsächlich in Verbindung mit dem ESP eingesetzt, wodurch das originale Datenpaket in ein weiteres Paket verpackt und der ursprüngliche IP-Header geschützt wird.
Allerdings ist auch hier der Einsatz des AH möglich; einzeln bzw. In der gem. Nutzung mit dem ESP.

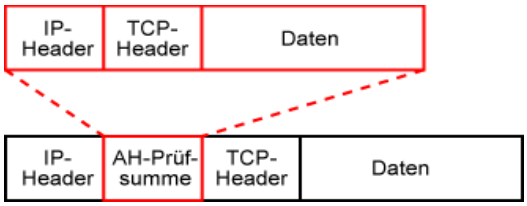


(Abb. 8: IP-Paket im Tunnelmodus)

3. Implementierungen / Protokolle / Anforderungen

- AH (Authentification Header)

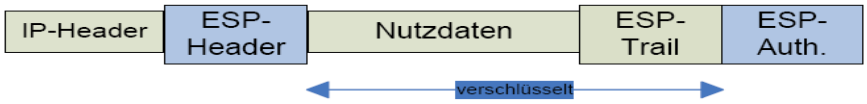
Der AH wird angewendet, um Herkunftsdaten und Inhalt der transportierten Daten vor unbemerkter Manipulation durch Dritte zu schützen. Hierbei wird über das gesamte IP-Paket ein Hashwert gebildet, der hinter dem ursprünglichen IP-Header eingefügt wird. Durch Überprüfung dieses Wertes kann der Empfänger nachträgliche Manipulationen an der Identität des Absenders sowie der Vollständigkeit und Korrektheit des Datenpaketes erkennen und dieses verwerfen.



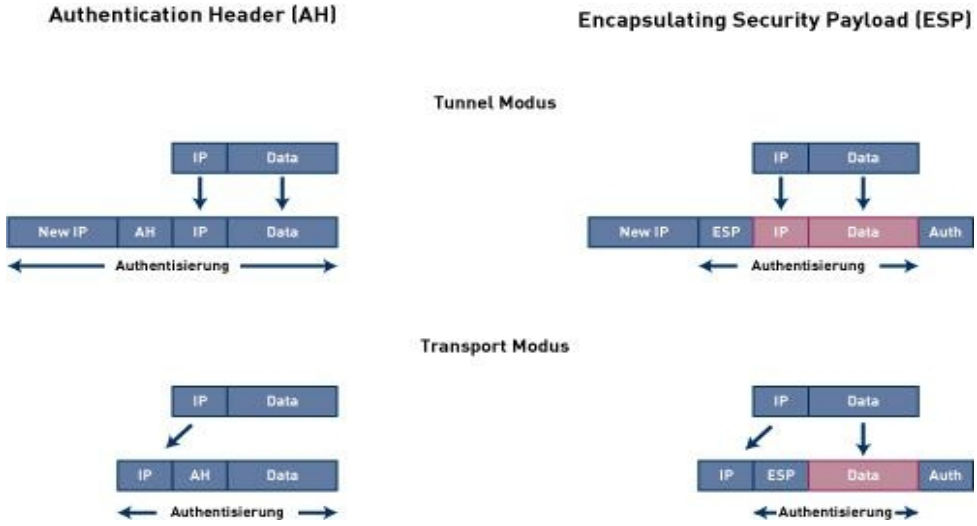
(Abb. 9: Authentification Header im Transportmodus, Quelle: http://www.elektronik-kompendium.de/)

- ESP (Encapsulating Security Payload)

Das ESP sorgt für Vertraulichkeit der Daten durch Verschlüsselung der Nutzdaten , dem sogenannten Payload oder des gesamten Datagramms.



(Abb. 10: ESP im Transportmodus, Quelle: http://www.elektronik-kompendium.de/)



(Abb. 11: zum besseren Verständnis der Arbeitsweise AH und ESP bzw. Des Tunnel- und Transportmodus, Quelle: UNBEKANNT)

3.2.3.2 SA, IKE, Zertifikate

- SA (Security Association)

  Die SA dient der Vereinbarung von Mechanismen und Algorithmen für das Hashing (umwandeln einer langen Eingabe in ein kurze Ausgabe) sowie der Authentifizierung zwischen den Kommunikationspartnern.
  All diese Parameter werden bei jedem Verbindungsaufbau neu ausgehandelt und dienen als Vertrauensstellung der Gegenstellen untereinander.

- IKE (Internet Key Exchange Protokoll)

  Das IKE-Protokoll nutzt standardmäßig 2 Phasen, die Erste zum Aushandeln einer SA (durch Aggressive Mode oder Main Mode) und die Zweite zur Erzeugung einer SA für IPSec (bzw. Andere Sicherheits-Protokolle) mittels Quick Mode.
  Es dient dem vertraulichen Verbindungsaufbau zwischen den Kommunikations-partnern, die keine Informationen des jeweils anderen besitzen.
  Desweiteren dient es der Schlüsselverwaltung für IPSec.
  IKE basiert u.a. Auf dem ISAKMP (Internet Security Association and Key Mangagement Protokoll).

  Aggressive Mode ist eine schnellere aber etwas unsichere Variante des Main Mode von IKE, da hierbei die Werte im Klartext übertragen werden.
  Eine kurze Abhandlung zum Ablauf des Main Mode bzw. des Aggressive Mode befindet sich im Anhang.

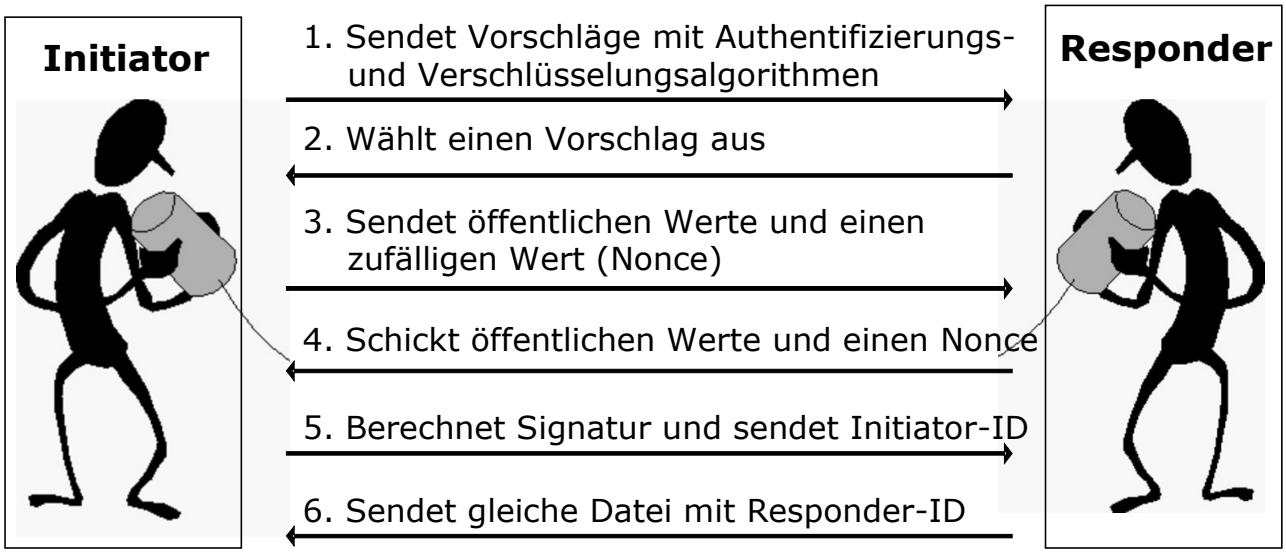
- Zertifikate

  Unter Zertifikaten wird eine digital signierte Erklärung einer Zertifizierungseinrichtung verstanden, die nachweist, dass ein öffentlicher Schlüssel zu einem benannten Teilnehmer gehört.

< Anhang >

A. MAIN MODE

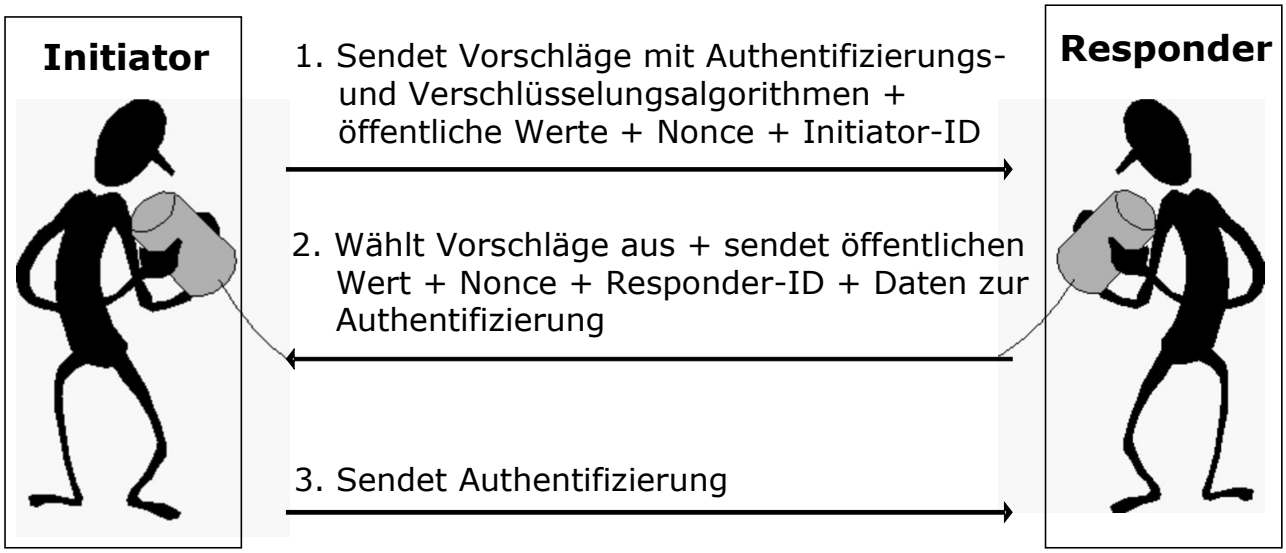
MAIN MODE Aushandeln einer SA durch 6 Nachrichten



(Abb. 12: Ablauf Main Mode, Quelle: www.inf.fu-berlin.de*)*

B. AGGRESSIVE MODE

AGGRESSIVE MODE Aushandeln einer SA durch 3 Nachrichten



(Abb. 13: Ablauf Aggressive Mode, Quelle: www.inf.fu-berlin.de*)*