

# **White Paper**

## **Multicast Anwendungen auf Basis von IPSec**

Autor: Erik Neumann

Der Inhalt dieses Dokumentes würde gleichlautend im Tagungsband des 8. Deutschen IT-Sicherheitskongresses des BSI (Bonn, 13. Bis 15. Mai 2003) veröffentlicht. Für den mit gleichem Inhalt gehaltenen Vortrag erhielt Herr Erik Neumann den 2. Preis beim abschließenden „Best Paper Award“.

# Multicast Anwendungen auf Basis von IPSec

Erik Neumann, media transfer AG, Darmstadt

IP Multicast und IPSec sind zwei etablierte Technologien mit unterschiedlichen Zielsetzungen: IP Multicast reduziert die notwendige Bandbreite beim Versand des gleichen Inhalts an viele Adressaten und IPSec sichert IP Datenströme ab. Die Kombination beider Technologien würde also den gesicherten Versand an viele Teilnehmer erlauben. Anwendungsszenarien wären z.B. vertrauliche Telefonkonferenzen oder Pay-TV. Je nach Sicht und Vorwissen des Lesers geht es um diesem Beitrag daher um die Absicherung von IP Multicast oder um die Erweiterung von IPSec.

## 1 Grundlagen IP Multicast

Bei traditionellem IP Unicast werden Pakete von einem Sender zu einem Empfänger transportiert. Dieses Verfahren benötigt insbesondere serverseitig sehr viel Bandbreite, wenn die gleichen Pakete an viele Empfänger gesendet werden müssen.

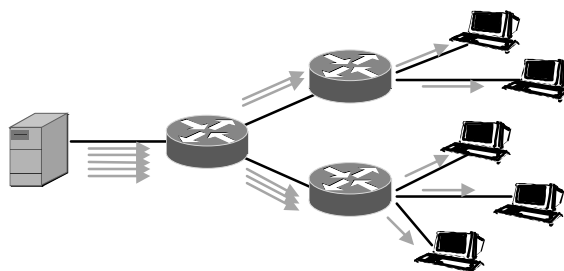


Abbildung 1: IP Unicast

IP Multicast reduziert die Netzlast, indem Pakete erst am letztmöglichen Knoten dupliziert werden.

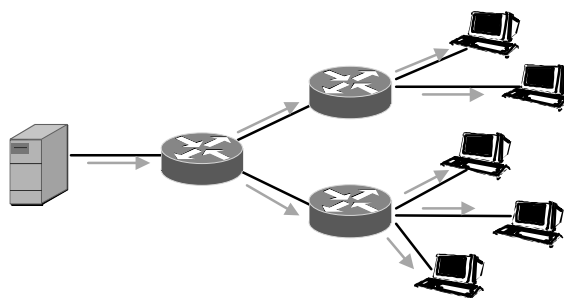


Abbildung 2: IP Multicast

Wie Abbildung 2 schon verdeutlicht gibt es bei IP Multicast drei verschiedene Rollen:

- **Sender:** Der Sender verschickt ein Multicast Paket genau einmal. Die Besonderheit ist nur die Zieladresse, die das Paket als Multicast Paket kennzeichnet.
- **Empfänger:** Damit ein Multicast Paket einen Empfänger erreicht, muss dem Netzwerk bekannt sein, dass der Empfänger an Paketen mit dieser Zieladresse interessiert ist. Der Empfänger muss dazu dem nächstgelegenen Router sein Interesse an Paketen mit einer bestimmten Multicast Adresse signalisieren.
- **Router:** Die Router haben die komplizierte Aufgabe festzustellen, welche Pakete an welche Schnittstellen weitergeleitet werden müssen. Wie auch bei IP Unicast hängt die Entscheidung von der Zieladresse ab. Ein Multicast Router muss also je Zieladresse speichern an welche Schnittstelle Empfänger angeschlossen sind. Gegenüber anderen Routern muss er sich aber selbst wie ein Empfänger verhalten.

Aus diesem Ansatz ergeben sich direkt einige wichtige Eigenschaften von IP Multicast:

- Das Netz regelt die Verteilung der Pakete, d.h. es werden keine Anforderungen an den Server gestellt, die über IP Unicast hinausgehen. Insbesondere muss der Sender das IP Multicast Protokoll IGMP (Internet Group Management Protocol, RFC2236) nicht implementieren.
- Die Empfänger und alle dazwischen liegenden Router müssen IGMP implementieren, um den benachbarten Routern das Interesse an Multicast Paketen zu signalisieren. Wenn Teile des Netzwerkes kein Multicast unterstützen, besteht allerdings die Möglichkeit die Multicast und IGMP Pakete durch Unicast Tunnel zu senden.
- Sender dürfen auch Empfänger sein und umgekehrt. So sind z.B. Konferenzsysteme realisierbar. Insbesondere darf (und soll) es für einzelne IP Multicast Gruppen (entspricht einer IP Multicast Adresse) mehrere Sender geben.
- Die Menge der Teilnehmer an einer Multicast Sitzung ist dynamisch. Während die Sitzung läuft, können Teilnehmer der Sitzung beitreten oder die Sitzung verlassen. Insbesondere ist die Menge der Teilnehmer zu Beginn der Sitzung gar nicht bekannt.
- IP Multicast selbst sieht keine Empfangsbestätigung vor. Verbindungslose Protokolle wie UDP lassen sich über IP Multicast betreiben. Bei verbindungsorientierten Protokollen wie TCP bestehen aber Probleme mit den Empfangsbestätigungen und der Wiederholung verlorener Pakete. „Reliable Multicast“ ist daher immer noch ein Forschungsthema.
- Die fehlende Kontrolle der Empfänger ist nicht nur ein Problem der Zuverlässigkeit der Übertragung. Ein weitere Folge ist auch die mangelnde Sicherheit. Prinzipiell kann der Sender nämlich auch die Gruppe der Empfänger nicht effektiv einschränken. Damit ist IP Multicast für Lauschangriffe noch anfälliger als IP Unicast.

Typische Anwendungen für IP Multicast sind

- Audio/Video Ausstrahlung: Fernsehen, Vorträge, Ansprachen, ..
- Push Medien: News Ticker, Wetter- und Stau-Meldungen, Sport Ergebnisse, ..
- Dateiverteilung: Abgleich von Datenbanken oder Web-Servern, Updates, Caching, ..
- Signale: Zeit, Multicast Sitzungsdaten, Zufallszahlen, Standort mobiler Geräte, ..
- Überwachung: Börsenkurse, Zustand von Netzkomponenten, Sensoren, Kameras, ..
- A/V Konferenzen mit oder ohne zentralen Server
- Fernunterricht: A/V Ausstrahlung erweitert um Unterlagenversand oder Interaktion

Aktuelle Betriebssysteme für Endgeräte unterstützen ebenso wie die kommerziell verfügbaren Router das Multicast Protokoll IGMP. Einer flächendeckenden Einführung steht also nicht die Technologie im Wege. Das Hindernis ist stattdessen die Problematik der Abrechnung zwischen verschiedenen Netzbetreibern. Schließlich ist bei einem eingehenden IP Multicast Paket der Aufwand zur Weiterleitung nicht einfach zu bestimmen.

## 2 Grundlagen IPSec

IPSec ist das umfangreichste Sicherheitsprotokoll für IP. Kurz gesagt ist IPSec eine VPN-Technologie, die sichere Tunnel über unsichere Netze etabliert. IPSec stellt Mechanismen für alle gängigen Sicherheitsanforderungen bereit. Die Besonderheit von IPSec ist aber seine Flexibilität. Funktionalitäten lassen sich gemäß der Anforderungen aktivieren oder deaktivieren. Für die Verschlüsselung und Authentifizierung können sogar die Algorithmen ausgewählt werden.

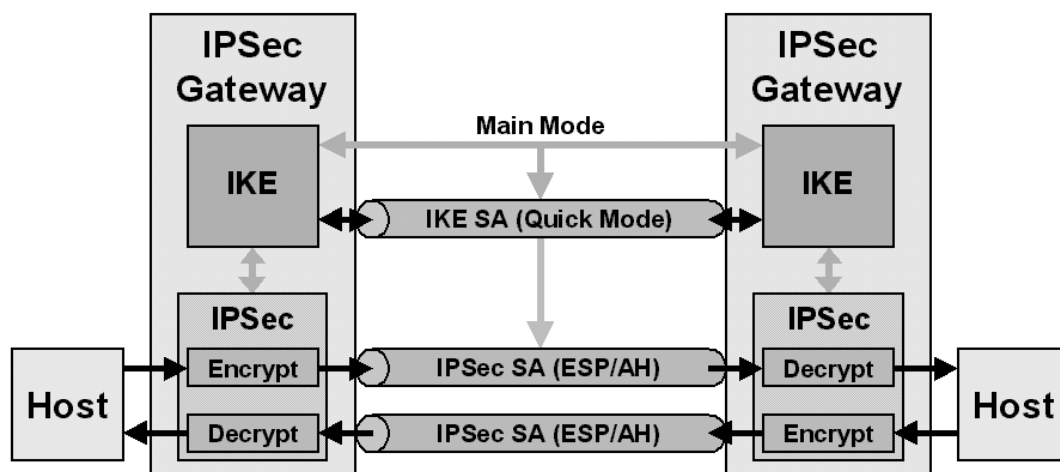
Üblicherweise wird IPSec verwendet, um private Netze über öffentliche Netze hinweg sicher zu verbinden. Dazu wird jedes der privaten Netze über ein IPSec Gateway mit dem öffentlichen Netz verbunden. Die Gateways bauen dann bei Bedarf untereinander sichere Tunnel auf. Host Implementierungen sind ebenfalls möglich, kommen aber meist nur im privaten Bereich oder bei mobilen Nutzern zum Einsatz. Die Verwendung von Gateways hat den Vorteil, dass außer den Gateways keine Komponente von den Tunneln wissen muss. D.h. die Verwendung von IPSec ist für den Sender, den Empfänger und für alle dazwischen liegenden Knoten (außer den Gateways) transparent.

Was die Sicherheit von IPSec betrifft, bestehen keine ernsthafte Bedenken. Allerdings gibt es andere Kritikpunkte. Erstens ist die Zahl der Tunnel unter Umständen sehr groß. Bei 20 Teilnehmern kann es zum Beispiel bis zu 190 Tunnel geben. Teilt man den Traffic je nach Sicherheitsanforderungen auf verschiedene Tunnel auf, kann die Zahl sogar noch deutlich größer sein. Die Anforderungen an die Bedienbarkeit und Strukturierung der Management Software sind also sehr hoch.

Zweitens ist der IPSec Standard sehr umfangreich und auf mehrere RFCs verteilt. Die Trennung der Beschreibung ist nicht immer auf den ersten Blick einleuchtend. Außerdem ist der Standard trotz seines Umfangs nicht in jeder Hinsicht eindeutig, d.h. es gibt an einigen Stellen Interpretationsspielräume. Als Folge dieser Komplexität und wegen der Flexibilität des Standards, ist Interoperabilität nicht selbstverständlich. Gerade bei großen, heterogenen Netzen kann sie teilweise ohne den Verzicht auf bestimmte Funktionalitäten überhaupt nicht erreicht werden.

Die Konfiguration eines IPSec Gateways ähnelt in bestimmten Aspekten der einer Firewall (Paket-Filter). Je Quelladresse, Zieladresse, Schnittstelle, Protokoll, Port usw. wird definiert, ob das Paket verworfen oder weitergeleitet wird. Bei einem IPSec Gateway kommt als dritte Möglichkeit der Versand durch einen Tunnel in Frage. Für diesen Fall müssen die Parameter des Tunnels definiert werden. Der wichtigste Parameter ist natürlich die Adresse des Ziel-Gateways.

Wenn ein Paket durch einen Tunnel geschickt werden muss, der noch nicht besteht, nimmt das Gateway Kontakt zum entsprechenden Ziel-Gateway auf. Im sogenannten Main Mode sendet es zuerst seine Vorschläge über die Parameter des Tunnels. Das empfangende Gateway sucht sich einen Vorschlag aus und sendet diesen zurück. Anschließend werden Informationen für die Authentifizierung der Gateways und die Einigung auf einen gemeinsamen Schlüssel (Diffie-Hellman Algorithmus) übertragen. Als Alternative zum Main Mode kann auch der Aggressive Mode verwendet werden, der annähernd die gleiche Funktionalität bietet, aber mit weniger Paketen auskommt.



**Abbildung 3: Aufbau von IPSec**

Tunnel heißen in der Terminologie von IPSec Security Associations (SAs). Das Ergebnis von Main oder Aggressive Mode ist die IKE SA (Internet Key Exchange, RFC2409), die manchmal auch ISAKMP SA (Internet Security Association and Key Management Protocol, RFC2408) oder äußere SA genannt wird.

Die IKE SA ist allerdings nicht der Tunnel, durch den die zu sichernden Pakete verschickt werden. Stattdessen wird die IKE SA nur verwendet, um mittels des sogenannten Quick Mode die IPSec SAs (oder inneren SAs) auszuhandeln. Die zu

verschlüsselnden Pakete werden dann mit den Protokollen ESP (Encapsulating Security Payload, RFC2406) und/oder AH (Authentication Header, RFC2402) durch die IPSec SAs verschickt.

Die Aufteilung auf zwei verschiedene Typen von Tunnel ist einer der Gründe für die Komplexität von IPSec. Allerdings bietet die Trennung auch Vorteile. Erstens ist der Quick Mode sehr schnell, weil keine Authentifizierung mehr nötig ist. Zweitens kann der Schlüssel, der im Main Mode für den äußeren Tunnel ausgehandelt wurde, lange Zeit benutzt werden, weil nur sehr wenig Pakete damit verschlüsselt werden. Die Lifetime der IKE SA kann also wesentlich höher sein als die Lifetime der IPSec SAs. Schließlich kann die IKE SA auch „auf Verdacht“ aufgebaut werden, um die Etablierung von Tunneln bei Bedarf zu beschleunigen.

### 3 IPSec und Multicast

Versucht man IPSec auf IP Multicast zu übertragen, so ergeben sich einige Probleme, die hier kurz erläutert werden sollen.

1. Tunnel Identifikation: IPSec verwendet einen sogenannten Security Parameters Index (SPI) zur Zuordnung von eingehenden Paketen zu Tunneln. Bei IPSec wird die SPI durch den Empfänger vergeben. Da die Empfänger zu Beginn der Sitzung nicht feststehen, ein einzelnes Paket mehrere Empfänger haben kann und zu Beginn der Sitzung vielleicht noch gar keine Empfänger vorhanden sind, kann bei Multicast IPSec die SPI nur durch den Sender oder durch eine unabhängige, verfügbare, zentrale Instanz vergeben werden.

Das Problem der SPIs lässt sich dadurch lösen, dass eine IPSec Implementierung eingehende Pakete nicht nur anhand der SPI einem Tunnel zuordnet, sondern die Kombination aus Zieladresse und SPI verwendet. Dies erfordert eine Änderung der internen Tabellen der Implementierung. Weiterhin müsste natürlich das Protokoll dahingehend angepasst werden, dass die SPI vom Sender zugewiesen wird.

2. Sequenz Nummern: Bei einer Replay Attacke sendet ein Angreifer ein mitgehörtes Paket. Dazu muss der Angreifer den Inhalt des Pakets nicht unbedingt verstanden haben. Es genügt schon, dass er die Wirkung des Pakets verstanden hat. Wenn er das Paket erneut schickt, kann er die Wirkung wiederholen. Zur Abwehr von Replay Attacken nummerieren die IPSec Protokolle die Pakete durch. Diese Sequenz Nummern sind aufsteigend, so dass alte Pakete erkannt und verworfen werden können. Bei Multicast Sitzungen kann es aber mehrere Sender geben. Für Multicast IPSec müssten die Sender die Sequenz Nummern untereinander synchronisieren.

Das Problem der Sequenz Nummern tritt erst auf, wenn mehrere Sender beteiligt sind. Eine mögliche Lösung (neben dem Verzicht auf die Auswertung der Sequenz Nummern) ist die Auswertung der Sequenz Nummern je Sender. Die Implementierung dieser Lösung bedeutet aber einen tiefen Eingriff in bestehende

IPsec Realisierungen, weshalb sich viele Bemühungen zur Spezifikation oder Realisierung von Multicast IPsec vorerst nur auf einen Sender beschränken.

3. Diffie-Hellman: Der Diffie-Hellman Algorithmus, den IPsec bei der Etablierung der IKE SA verwendet, ermöglicht zwei Parteien die Einigung auf einen gemeinsamen Schlüssel, ohne dass dieser Schlüssel explizit übertragen werden muss. Dazu schickt jeder Teilnehmer einen Anteil. Beide Parteien können daraus den gemeinsamen Schlüssel errechnen, ein Zuhörer allerdings nicht. Leider lässt sich der Algorithmus nicht einfach von zwei auf mehr Parteien erweitern. Außerdem sind bei einer Multicast Sitzung die Teilnehmer nicht im Vorfeld bekannt und verfügbar. Daher muss die Festlegung des gemeinsamen Schlüssels für Multicast IPsec auf andere Weise erfolgen.

Dies ist das Hauptproblem von Multicast IPsec. Die offensichtliche Lösung besteht darin, dass eine zentrale Instanz die Schlüssel generiert und verteilt. Mögliche Teilnehmer einer Multicast Sitzung müssen sich gegenüber der zentralen Instanz authentifizieren und erhalten daraufhin von ihr die aktuellen Schlüssel. Die Anmeldung ist sowohl für Sender als auch für Empfänger notwendig.

#### 4 Standardisierung

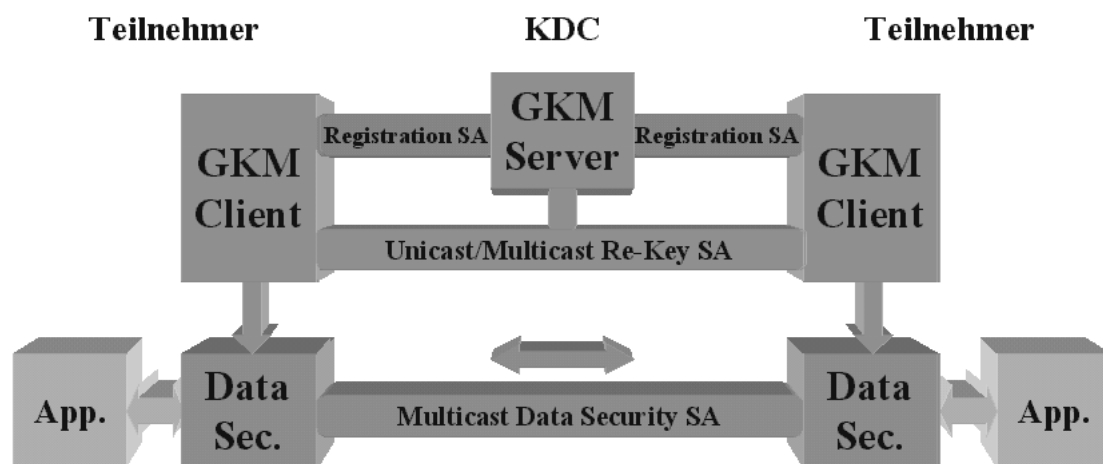
Die Internet Engineering Task Force (IETF) ist das Standardisierungsgremium rund um das Internet Protocol (IP). Innerhalb der IETF gibt es sogenannte Working Groups (WGs), die sich mit unterschiedlichen Themen beschäftigen. Eine WG mit dem Namen Multicast Security (MSEC) hat sich die Sicherung von IP Multicast zum Ziel gesetzt. Ausgangspunkt für die meisten Aktivitäten ist die Anpassung oder Erweiterung von IPsec für eben diesen Zweck.

Den meisten Internet Standards gehen Forschungsarbeiten der weniger bekannten Internet Research Task Force (IRTF) voraus. Die IRTF ist in Research Groups (RGs) gegliedert. Eine RG heißt Group Security (GSEC, früher Secure Multicast Group, SMuG). Die Arbeiten dieser Gruppe sind wesentliche Vorlagen der Standardisierungsbemühungen der MSEC WG.

MSEC hat bisher keine Request for Comments (RFCs) veröffentlicht. Es gibt allerdings einige sehr stabile und vielversprechende Drafts. Leider ist die Gliederung der Dokumente ähnlich kompliziert wie beim „traditionellen“ IPsec. Als Basis kann das Dokument „Group Key Management Architecture“ angesehen werden, das die Konzepte und den möglichen Aufbau von Multicast IPsec beschreibt. Das Dokument beschreibt stattdessen die Akteure und ihre Aufgaben. Es werden die notwendigen Protokolle identifiziert und deren Funktionalität beschrieben. Teilweise enthält das Dokument auch Vorschläge für die Realisierung der Protokolle, jedoch keine Spezifikationen. Die aktuelle Arbeit der MSEC WG besteht darin, in separaten Dokumenten Spezifikationen für die verschiedenen Protokolle zu erstellen.

Der Kern von Multicast IPsec ist der Einsatz einer zentralen Komponente für die Erstellung und Übertragung von Schlüsseln und für die Authentifizierung von

Teilnehmern. Diese Komponente ist das Key Distribution Center (KDC). Das KDC implementiert ein Group Key Management Protocol (GKMP). Jeder Teilnehmer, sei er Sender oder Empfänger, muss ebenfalls als GKM Client (GKMC) mit dem KDC als GKM Server (GKMS) kommunizieren. Genau wie die Schlüssel können bei dynamischen Gruppen auch die Eigenschaften der Tunnel (Algorithmen, Lifetime, ..) nicht mehr ausgehandelt werden. Das KDC muss über das GKMP neben den Schlüsseln also auch die Eigenschaften der Tunnel verteilen. Das folgende Diagramm veranschaulicht das Konzept für Multicast IPsec:



**Abbildung 4: Konzept für Multicast IPsec**

Für die Übertragung der Konzepte von (Unicast) IPsec auf die Anforderungen von IP Multicast war es notwendig, die Aufgaben der Protokolle genau zu unterscheiden. Der IKE Main Mode dient der Authentifizierung der Teilnehmer, der Definition eines Tunnels (IKE SA) für die weitere Kommunikation sowie der Einigung (Diffie-Hellman) auf den Schlüssel dieses Tunnels.

Der IKE Quick Mode wird durch den Tunnel gesichert, der im Main Mode definiert wurde. Der Quick Mode dient der Definition des eigentlichen Tunnels (IPsec SA) sowie der Übertragung der Schlüssel für diesen Tunnel.

Für Multicast IPsec wurde diese Gliederung beibehalten. Allerdings wurden zur Klarstellung der Funktionalitäten und zur Unterscheidung von Unicast IPsec neue Begrifflichkeiten eingeführt.

- Die Data Security SA ist ein Multicast Tunnel, durch den die Multicast Pakete gesichert werden. Er entspricht der IPsec SA von Unicast IPsec. Tatsächlich können (mit leichten Modifikationen) mit ESP und AH die gleichen Protokolle eingesetzt werden. Der Schlüssel für die Data Security SA heißt Traffic Encryption Key (TEK).
- Die Re-Key SA ist ein Tunnel, durch den der TEK an die Teilnehmer verteilt wird, d.h. er entspricht in seiner Funktionalität im wesentlichen der IKE SA von Unicast IPsec. Die Re-Key SA kann auf Multicast oder Unicast basieren. Die Re-Key SA

wird durch den Key Encryption Key (KEK) gesichert. Neue KEKs können ebenfalls durch die Re-Key SA übermittelt werden.

- Die Registration SA ist ein Tunnel, durch den die Teilnehmer initialen Zugang finden. Der Hauptzweck ist also die gesicherte Übermittlung des aktuellen KEK. Das Registration Protokoll muss dazu den Teilnehmer authentifizieren, einen gesicherten Tunnel etablieren und den KEK durch den Tunnel übertragen. Wie bereits erwähnt, wird neben dem KEK auch eine Reihe von Informationen übertragen, die die Re-Key SA und die Data Security SA beschreiben.

Der wesentliche Unterschied zwischen Unicast IPsec und Multicast IPsec ist also die Einführung des KDC und die damit einhergehende zentrale Definition und Verteilung von Schlüsseln und Tunnel-Parametern statt der bilateralen Aushandlung.

## 5 MuSeGa

MuSeGa steht für Multicast Security Gateway. Das System stellt eine Implementierung der oben beschriebenen Architektur dar. Parallel zu den Standardisierungsbemühungen der MSEC WG wurde ein Prototyp entworfen und entwickelt, der in der Lage war Multicast Traffic zu sichern. Der Prototyp basierte bereits auf IPsec und entsprach in seinem Aufbau ungefähr der einfachsten Form, die gemäß der MSEC Architektur erlaubt ist:

- Als Registration Protokoll wurde OpenSSL eingesetzt. Die Teilnehmer wurden X.509 Zertifikate authentifiziert. Auf dem KDC befand sich eine „White List“ zur Definition der erlaubten Teilnehmer.
- Es gab keine Re-Key SA und kein Re-Key Protokoll. Zum Austausch des KEK mussten sich die Teilnehmer also erneut beim KDC anmelden. Ein Automatismus für diesen Vorgang war aber bereits implementiert.
- Als Data Security Protokoll wurde IPsec/ESP eingesetzt.
- Es gab nur einen Multicast Sender, der über UDP/RTP einen A/V-Strom verschickte. Das KDC befand sich auf dem gleichen Server, so dass der Sender sich den KEK nicht über das Registration Protokoll holen musste.

Der Prototyp war eine Art „Proof of Concept“, der beweisen sollte, dass das Konzept von Multicast IPsec funktionsfähig ist. Mit der Realisierung wurde bereits vor der Veröffentlichung der MSEC Architektur begonnen.

Die Nachteile dieses Prototypen sind offensichtlich:

- Eine Neu-Anmeldung bei jedem Wechsel des KEK ist ineffektiv und nicht skalierbar.
- Die Integration von Sender und KDC schränkt die Anwendung wesentlich ein. A/V-Server sind in der Praxis oft geschlossene Systeme, die ohne weiteres nicht um Sicherheitssoftware ergänzt werden können. Außerdem kann der

Rechenaufwand für die Verschlüsselung auch auf Kosten der eigentlichen Funktionalität als Streaming Server gehen.

- Der Prototyp bot keine Flexibilität bzgl. der verwendeten Protokolle und Algorithmen.
- Es gab keine Administrationswerkzeuge.

Die Weiterentwicklung verfolgte die Behebung dieser Nachteile und sollte ein System mit Produktreife zur Folge haben. Die wesentlichen Ideen waren:

- Trennung des KDC vom Multicast Sender
- Etablierung einer Re-Key SA
- Verwaltung von Sitzungsdaten in einer Datenbank des KDC
- Administrationswerkzeuge für den Zugriff auf die Datenbank
- Integration von KDC und GKM Client zum Multicast Security Gateway (MuSeGa)
- Unterstützung verschiedener IPSec Implementierungen für das Data Security Protocol
- Unterstützung verschiedener Re-Key Protokolle
- Einfache Integration in den Client (Zielformat MS Windows®)

Der Aufbau von MuSeGa wird im folgenden Diagramm veranschaulicht:

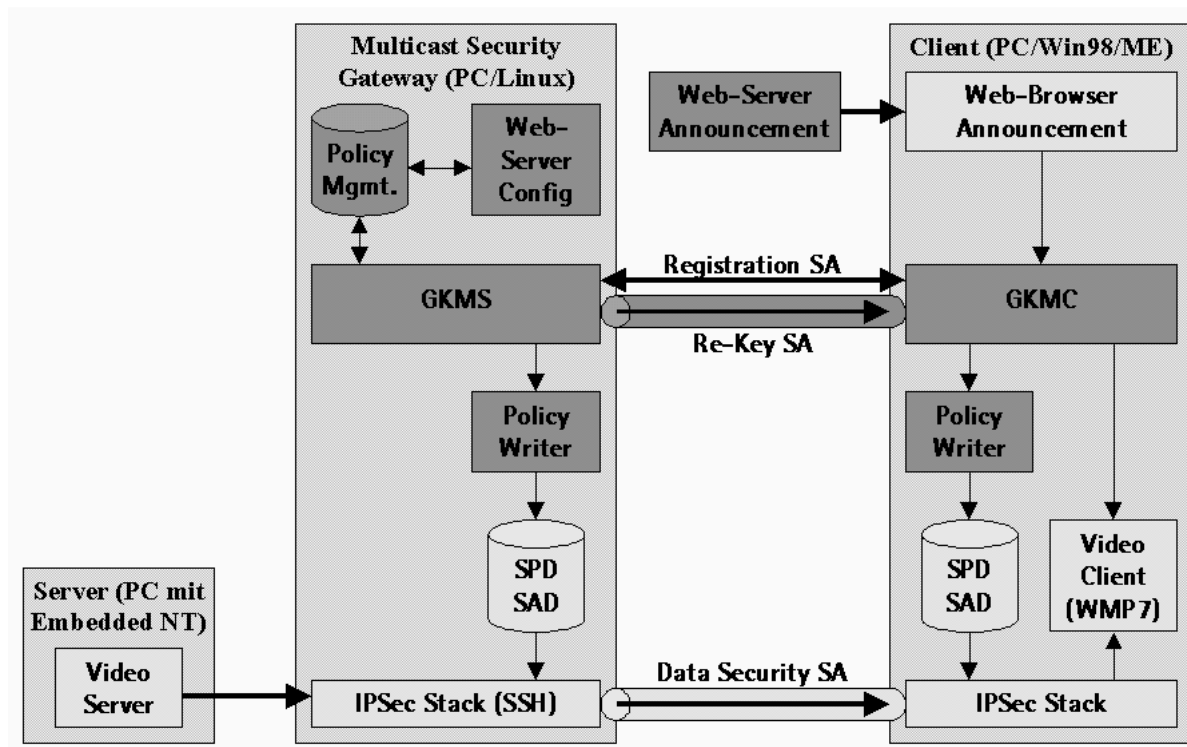


Abbildung 5: Multicast Security Gateway (MuSeGa)

## 6 Ausblick

Der schwierigste Bestandteil des Multicast IPsec Konzepts ist das Re-Key Protokoll. Hier gibt es ganz unterschiedliche Ansätze. Eine generelle Entscheidung zugunsten eines bestimmten Protokolls ist aber nicht möglich, weil jedes Protokoll seine Vor- und Nachteile hat. Daher muss die Entscheidung fallweise abhängig von den besonderen Eigenschaften der Anwendung getroffen werden. Das MuSeGa System trägt diesem Umstand dadurch Rechnung, dass je nach Sitzung verschiedene Re-Key Protokolle verwendet werden können. Über eine definierte Schnittstelle können weitere Protokolle integriert werden. Momentan sind zwei grundsätzliche verschiedene Re-Key Protokolle realisiert.

Re-Key Protokolle lassen sich nach folgenden Eigenschaften charakterisieren:

- Separate oder allgemeine KEKs: Prinzipiell ist es möglich (und erlaubt) für jeden Teilnehmer einen anderen KEK zu verwenden. Die Re-Key Nachrichten werden also „personalisiert“. Der Vorteil besteht darin, dass KEKs ausgetauscht werden können, ohne dass andere Teilnehmer den neuen KEK mitlesen können. Der offensichtliche Nachteil ist die Tatsache, dass jede Re-Key Nachricht an jeden Teilnehmer einzeln abgeschickt werden muss.
- Unicast oder Multicast: Unicast Re-Key Protokolle verschicken Re-Key Nachrichten an jeden Teilnehmer einzeln. Sie können dabei von verbindungsorientierten Protokollen wie TCP profitieren. Multicast Protokolle hingegen reduzieren die Bandbreiten, beinhalten aber keine Empfangsbestätigungen und müssen daher den Empfang des aktuellen KEK oder TEK auf andere Weise sicherstellen.
- Schlüsselerzeugung: Es gibt Re-Key Protokolle, die auf Algorithmen beruhen, die eine Aushandlung von Schlüsseln durch mehr als zwei Teilnehmer erlauben. Grob gesagt sind solche Algorithmen eine Erweiterung des Diffie-Hellman Algorithmus. Ein Beispiel ist die Logical Key Hierarchie (LKH). Die dazugehörigen Protokolle sind kompliziert und kompensieren nur schlecht Paketverluste und Teilnehmer, die einfach nicht mehr antworten (Nutzer hat Programm hart beendet). Ihr Vorteil liegt jedoch in der schnellen und effizienten Neuaushandlung von Schlüsseln, ohne dass ehemalige Teilnehmer den neuen Schlüssel erhalten.

Unicast Re-Key Protokolle können ihre Vorteile ausspielen, wenn sie auf Basis von TCP separate Schlüssel benutzen. Multicast Protokolle verwenden üblicherweise gemeinsame Schlüssel. Ohne den Einsatz von LKH und ähnlichen Algorithmen, können mit solchen Multicast Protokollen Teilnehmer aber nicht ausgeschlossen werden, da sie neue KEKs weiterhin empfangen können.

Für die Entscheidung für oder gegen ein Re-Key Protokoll müssen also folgende Fragen geklärt werden:

- Wie viele Teilnehmer hat die Sitzung maximal?
- Wie dynamisch ist die Gruppe der Teilnehmer, d.h. wie oft kommen Teilnehmer hinzu oder verlassen die Gruppe?
- Ist es notwendig, dass ehemalige Teilnehmer den weiteren Traffic nicht mehr entschlüsseln können?
- Ist es notwendig, dass neue Teilnehmer den vorangegangenen (evtl. aufgezeichneten) Traffic nicht entschlüsseln können?
- Wie viel Bandbreite steht den Teilnehmern neben dem eigentlichen Multicast Traffic zur Verfügung?

**Kontakt:**

Erik Neumann

Media transfer AG

Dolivostrasse 11

64293 Darmstadt

Tel.: +49 6151 / 8193-0

Fax.: +49 6151 / 8193-43

Mail: [contact@mtg.de](mailto:contact@mtg.de)