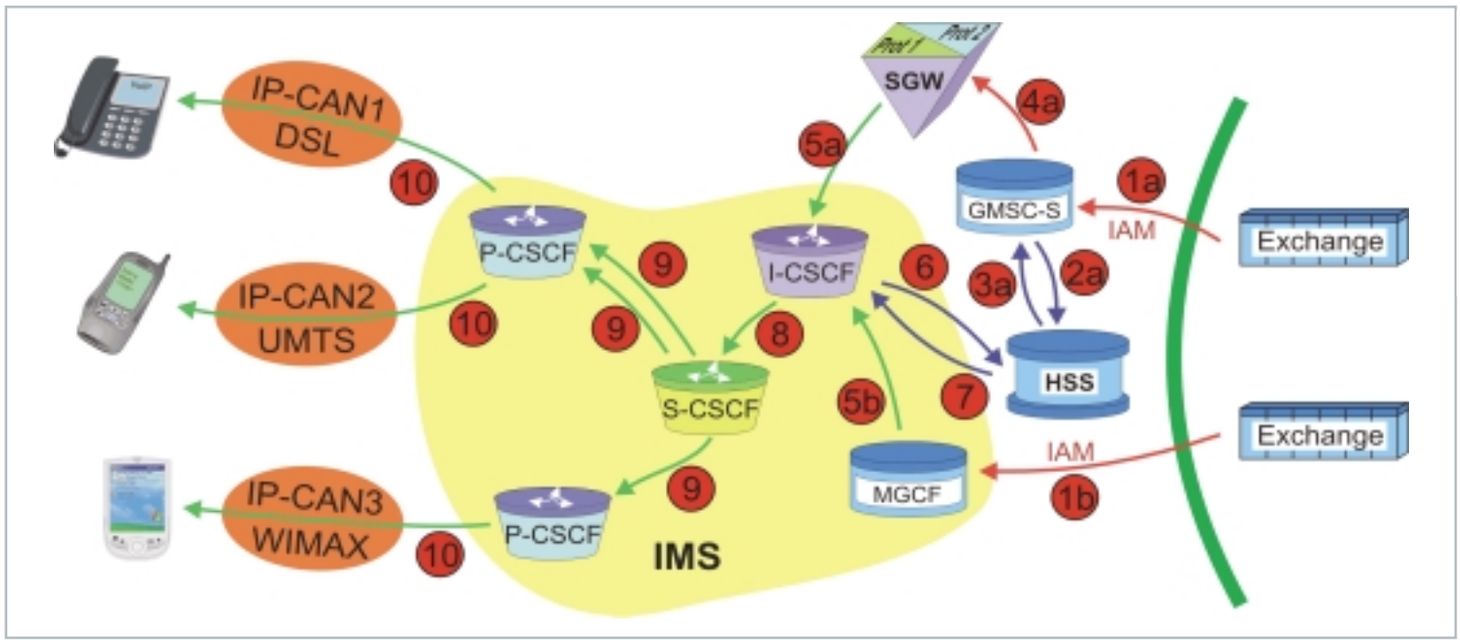
Hoffnungsträger IMS

Von Gunnar Heine

Noch sind einige Stolpersteine auf dem Weg zu einem großräumigen Einsatz des IP Multimedia Subsystem zu beseitigen. Doch für die Probleme der Plattform zur Bereitstellung von IP-basierten Kommunikationsdiensten gib es bereits interessante Lösungsansätze. Diese sollen hier skizziert werden.



Quelle: Inacon GmbH

Bild 5: Mögliches Handling von hereinkommenden Gesprächen im IMS

Es soll an dieser Stelle betont werden, dass die vorgestellten Ansätze die Sichtweise und Praxiserfahrungen des Autors repräsentieren und nicht durch Standardisierungs-Gremien und schon gar nicht durch Herstellerinteressen beeinflusst wurden. Ergänzend muss betont werden, dass die vorgestellten Lösungsansätze keine Off-the-Shelf-Lösungen repräsentieren, sondern viel Raum für Diskussion lassen.

Bei den hereinkommenden Telefonaten geht es um reguläre Telefonanrufe aus dem öffentlichen Netz für Nutzer eines IMS. Wie im letzten Heft dargestellt, besteht das Problem darin, dass die hereinkommende Gesprächsanforderung nicht zum Teilnehmer durchgeleitet werden kann. Zum Verständnis der vorgeschlagenen Lösung muss zwischen verschiedenen IMS-Typen unterschieden werden:

Beim IMS vom Typ 1 handelt es sich um IMS-Installationen von Mobilfunkbetreibern, welche ihre Kunden kurzfristig nur teilweise, langfristig aber komplett über das IMS mit Diensten versorgen werden. Das zeitliche Element ergibt sich durch die Akzeptanz seitens des Kunden für neue Endgeräte, welche längerfristig nur noch VoIP für Telefonie unterstützen dürften. Bei einem IMS vom Typ 1 wählt der Anrufende die wohlbekannte E.213-Telefonnummer seines Anruf-Partners, beispielsweise die „+49-171-540-7090“. In diesem Fall handelt es sich um die Vorwahl eines bekannten deutschen Mobilfunk-Operators und entsprechend wird der Anruf vom PSTN zu einem Gateway-MSC (Gateway Mobile Switching Center) dieses Mobilfunk-Operators gelenkt (Punkt 1a in Bild 5).

Beim IMS vom Typ 2 handelt es sich um IMS-Installationen von Festnetzbetreibern und um so genannte Greenfield-Operatoren. Beiden gemeinsam ist das Fehlen von Gateway-MSCs. Anstatt dessen werden hier MGCFs (Media Gateway Control Function) verwendet. Allerdings entfällt die – relativ einfache – Routing-Entscheidung anhand der Vorwahl. Es muss die komplette gerufene Nummer ausgewertet werden.

Nehmen wir einmal das Fallbeispiel der Rufnummer „+49-721-957829-0“. Die Ver-

Gunnar Heine ist Geschäftsführer der Inacon GmbH, Buchautor und Lehrbeauftragter an der Fachhochschule Wilhelmshaven.

mittlungsstelle (Exchange) vor der IAM-Nachricht mit Punkt 1b (Bild 5) trifft die Entscheidung, diesen Anruf an die MGCF zu leiten.

Das Bild 5 ist zunächst als „entweder ..., oder ...“ zu verstehen. Implizit stellt Bild 5 aber auch die faszinierende Kombination von Festnetz- und Mobilfunk-Anbieter dar, der seinen Kunden auch auf dem Mobilgerät ruft, obwohl die Festnetznummer gewählt wurde und umgekehrt. Die technische Umsetzung (nicht die politische) ist übrigens eine der leichteren Übungen fürs

Quelle: Inacon GmbH

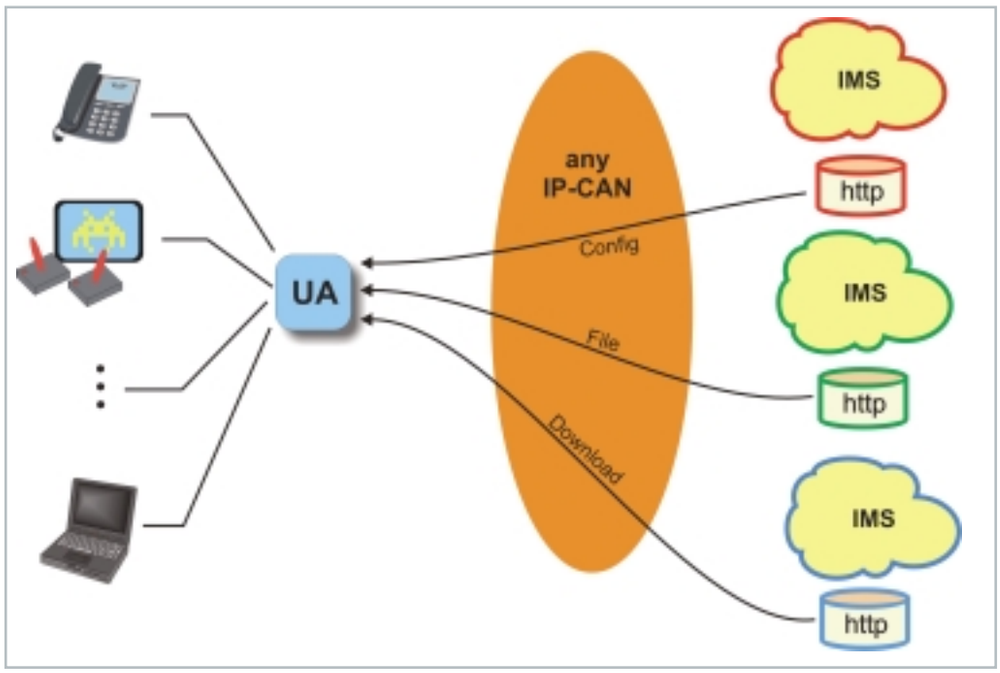


Bild 6: Adaptierung generischer Endgeräte ans IMS durch Konfigurations-Software

IMS. Das ganze wird als „Forking“ bezeichnet und ist in Bild 5 in den Punkten 9 und 10 beispielhaft dargestellt. Hier wird ein Nutzer auf drei Geräten gerufen, wobei die Registierung vom VoIP-Telefon und vom UMTS-Mobilgerät über dieselbe P-CSCF (Proxy Call Session Control Function) erfolgt sind. Daher gehen gleich zwei SIP:Invite-Nachrichten (Punkt 9) an die obere P-CSCF.

Zurück zur Ausgangs-Frage: Wie kommt der Anruf nun zum IMS-Nutzer? Im Moment befinden wir uns beim Gateway-MSC (Punkt 1a) beziehungsweise bei der MGCF (Punkt 1b). Dazu folgender Vorschlag, um die notwendigen Änderungen minimal zu halten:

Wie in Punkt 2a gezeigt, muss das GMSC (Gateway Mobile Switching Center) zunächst beim HSS (Home Subsriber Server) um Routing-Informationen nachsuchen. Für das GMSC ist dies nichts Neues. Die wohlbekannte MAP-Prozedur send RoutingInfo (muss tatsächlich so geschrieben werden) erledigt diese Aufgabe über das C-Interface schon seit der Einführung von GSM. Aber im Falle des Mobilfunkbetreibers schlägt hier die erste Änderung zu: Falls der gerufene Teilnehmer nur via IMS erreicht werden kann beziehungsweise primär über das IMS gerufen werden soll, gibt es im HSS keinen VLR-Eintrag (Visitor Location Register), was bei GSM- beziehungsweise UMTS-registrierten Teilnehmern der Fall wäre. Das HSS kann in diesem Fall also nicht beim VLR um Bereitstellung der so genannten MSRN (Mobile Station Roaming Number) nachsuchen, die in GSM-/UMTS-Netzen überhaupt erst die Weiterleitung des Anrufs ans „serving“ VLR ermöglicht.

Allzu problematisch ist dies letztlich aber nicht. Schon immer gibt es auch in GSM und UMTS nicht registrierte (abgeschaltete) Nutzer und für diese wird ein Anruf wahlweise auf die Sprachbox weitergeleitet. Es gibt demnach pro Nutzer-Profil im HSS unter anderem einen Eintrag für die zuständige Sprachbox. Die notwendige Änderung besteht nun darin, zusätzlich zum Sprachbox-Eintrag einen neuen Datenbank-Eintrag für die zuständige I-CSCF (Interrogating Call Session Control Function) im HSS vorzunehmen. Dies kann statisch geschehen, das heißt die I-CSCF beziehungsweise ihre Adresse (als „Host Name Address“) wird fest voreingestellt oder die Last wird zwischen verschiedenen I-CSCFs geteilt. Punkt 3a deutet an, wie die MAP:sendRoutingInfo-Antwort-Nachricht, die Identifikation der I-CSCF dem GMSC übergibt.

Die nächste Änderung ist über die mit Punkt 4 a gekennzeichnete Nachricht dargestellt: Das GMSC übergibt die IAM-Nachricht (Initial Address Message) zusammen mit der Adresse der I-CSCF an ein höchstwahrscheinlich internes SGW (Signaling Gateway), welches die E.213-Telefonnummer des Teilnehmers in einen so genannten TEL-URI umwandelt. Um unser Beispiel von vorhin fortzusetzen: Aus „+49-171-540-7090“ wird „tel: +49-171-540-7090“. Das SGW wandelt die ISUP:IAM-Nachricht mithilfe dieser Informationen in eine SIP:Invite-Nachricht um, die in Punkt 5a dargestellt wird.

An dieser Stelle müssen wir uns wieder einmal mit der b-Variante unten in Bild 5 beschäftigen. Auch die MGCF des Festnetzbetreibers beziehungsweise des Greenfield-Operators erhielt ja eine ISUP:IAM-Nachricht (Punkt 1b), allerdings für die E.213-Rufnummer „+49-721-957829-0“. Die MGCF benötigt keine HSS-Abfrage, sondern übersetzt von sich aus diese E.213-Rufnummer in einen TEL-URI und leitet die Anfrage an eine I-CSCF im IMS weiter. An dieser Stelle konvergieren die a- und die b-Variante und wir können ab Punkt 6 zu bereits im Standard beschriebenen Prozeduren zurückkehren. Beim Informationsaustausch Punkt 6 und 7 handelt es sich um die Diameter:LIR/LIA-Prozedur, welche in 3GTS 29.229 (6.1.5 und 6.1.6) beschrieben ist. Im Wesentlichen wird durch die I-CSCF und vom HSS die Adresse der S-CSCF (Serving Call Session Control Function) erfragt. Mithilfe dieser Information kann die I-CSCF die empfangene SIP:Invite-Nachricht für „tel: +49-171-540-7090“ beziehungsweise „tel: +49-721-957829-0“ an die zuständige S-CSCF routen (Punkt 8).

Die S-CSCF wertet aus, wo der Kunde registriert ist und leitet die SIP:Invite-Nachricht gleich an drei Endgeräte weiter, welche über zwei unterschiedliche P-CSCF's erreicht werden müssen (Punkt 9). Endlich erreicht der Ruf den Endkunden beziehungsweise dessen Endgeräte: Im dargestellten Fall (Punkt 10) klingeln alle drei Endgeräte gleichzeitig. Dies wird „Simultaneous Forking“ genannt. Alternativ können die drei Endgeräte auch nacheinander

gerufen werden, zum Beispiel mit 30 Sekunden Klingeln, bevor weitergeschaltet wird („Sequential Forking“). Dies muss in der S-CSCF konfiguriert werden.

Wie schon gesagt, handelt es sich hier um einen Vorschlag zur Lösung dieses Problems. Wir möchten nochmals ausdrücklich darauf hinweisen, dass dieser Vorschlag noch nicht standardisiert ist. Wir möchten aber auch auf einige Vorteile dieser Lösung hinweisen:

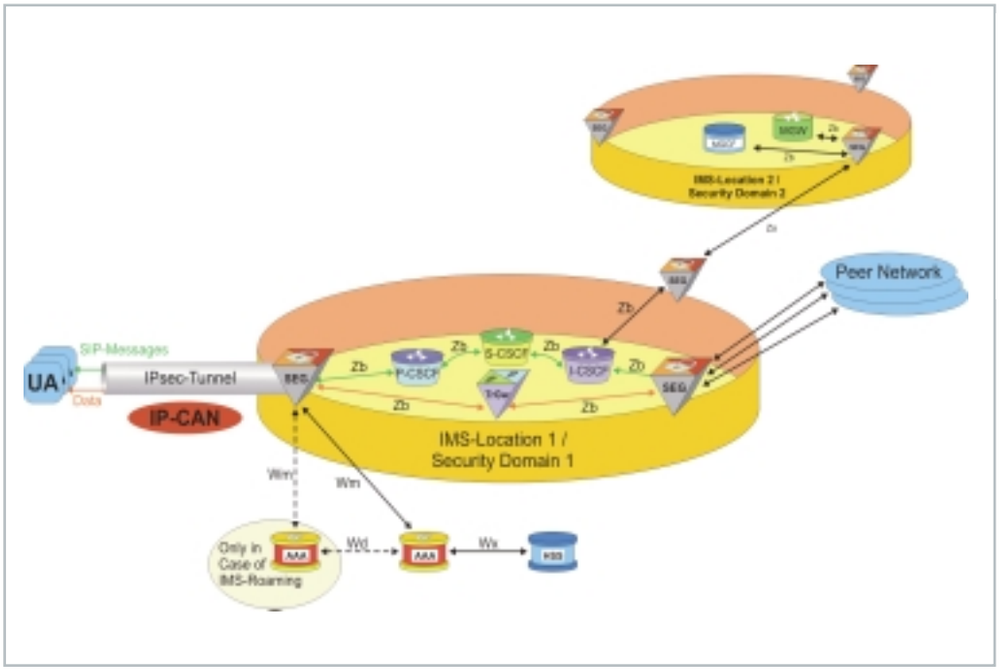
- Bereits am GMSC mit integriertem SGW wird von ISUP (ISDN User Part) auf SIP und damit auf IP umgeschaltet. Der nicht dargestellte Datenbereich für die eigentliche Sprache wird am zugehörigen MGW auf VoIP umgewandelt.
- Dieser Vorteil bekommt dann besonderes Gewicht, wenn eine so genannte „Hosted IMS“-Variante eingesetzt wird, bei der das IMS eines Betreibers geografisch und politisch ganz woanders ist als sein Netz.
- Die notwendigen Veränderungen an der bestehenden Architektur sind minimal. Für die I-CSCF erscheint die hereinkommende SIP:Invite-Nachricht wie jede andere VoIP-Gesprächsanforderung.

Lösungsansätze QoS und Zugangsnetze

Nochmal kurz zur Wiederholung: Das Problem der Verfügbarkeit von Echtzeit QoS im Zugangsnetz (IP-CAN) ergibt sich aus der Erwartung des Kunden heraus, Telefongespräche und andere Echtzeit-Dienste auch tatsächlich mit Echtzeit-Qualität nutzen zu können. Problem des Zugangs von jedem Zugangsnetz aus erschwert mögliche Lösungsansätze durch die gleichzeitige Erwartungshaltung des Kunden, IP-basierte Dienste auch von jedem IP-basierten Zugangsnetz aus verwenden zu können. Bestes Beispiel: Der Kunde kommt nach Hause und möchte sein WLAN-fähiges Mobiltelefon vom teuren GSM/GPRS aufs WLAN umbuchen und über WLAN angerufen werden können. Um es von vornherein ganz klar zu sagen: Für die beiden Probleme gibt es keine endgültige und saubere technische Lösung nach dem Prinzip der Problemlösung im ersten Beispiel.

Man kann aber einem Operator folgende Empfehlungen aussprechen, die das Problem nicht lösen sondern gar nicht erst aufkommen lassen:

- Gestatten Sie Ihren Kunden den Zugang von beliebigen Zugangsnetzen aus, nachdem Sie Ihre Gebührenstruktur entflochten haben.
- Diese Entflechtung muss eine Aufteilung der Kosten in puren Zugang (Access Network Charges) und Dienste (Service based Charges) beinhalten.
- Verwendet der Kunde nun ein Zugangsnetz des IMS-Operators mit „QoS-Awareness“, dann fallen entsprechend höhere Gebühren an als wenn das vorhandene „Best Effort“-WLAN/DSL-Netz von einem beliebigen ISP verwendet wird.
- Vorteil: Für einen möglichen Mangel an Qualität im letzteren Fall, kann der Kunde den IMS-Operator nicht verantwortlich machen.



Quelle: Inacon GmbH

Bild 7: IMS mit voll ausgebauter IPsec-Sicherheitsarchitektur

- Dieser Ansatz bedeutet nicht, dass ein IMS-Operator keine eigenen Zugangsnetze (mehr) betreibt. Er erlaubt aber, dass IMS-Service-Anbieter und Anbieter des oder der Zugangsnetze zwei getrennte juristische Einheiten sind.

Für den Betreiber ergeben sich aus dieser politischen Entscheidung die folgenden Vorteile:

- Dem Kunden gegenüber wird pro-aktives anstatt restriktives Verhalten signalisiert, was vom Markt immer honoriert wird.
- Dem Betreiber bleibt die Diskussion und Validierung ungezählter MoUs (Memorandum of Understanding) mit Zugangsnetz-Betreibern erspart, um deren QoS- und sonstigen Fähigkeiten sicherzustellen. Verwaltungs- und damit Kostenaufwendungen werden minimiert.

Es muss abschließend gesagt werden, dass ein IMS-Zugriff von beliebigen Zugangsnetzen aus noch andere Schwierigkeiten und Lücken im Sicherheitsbereich aufweist, auf die weiter unten getrennt eingegangen wird.

Lösungsansatz Interoperabilität

Das Problem Interoperabilität ergibt sich wie in den vorangegangenen Ausgaben dargestellt, aus der Installation von IMS-Lösungen mit zumindest proprietären Anteilen und Prozeduren sowie den beachtlichen Unterschieden zwischen den zugrunde liegenden Standards. Hier kann man unterscheiden zwischen den unterschiedlichen IMS-Standards wie zum Beispiel TISPAN, 3GPP, 3GPP2 und unterschiedliche Protokoll-Standards im Endgerätebereich. Der letzte Punkt adressiert insbesondere die Protokolle SIP und SDP (Session Description Protocol), welche sich zwischen dem generischen IETF-SIP/SDP und den verschiedenen IMS-SIP/SDP-Versionen beachtlich unterscheiden. Die entscheidenden Fragen sind zum Beispiel:

- Funktioniert mein Endgerät, welches ich ursprünglich beim Operator A betrieben habe, auch beim Operator B?
- Kann ich mein Endgerät über ein Zugangsnetz meines vorhergehenden Operators A an das IMS meines neuen Operators B anschließen?
- Können zwischen unterschiedlichen IMS-Implementierungen überhaupt Sessions aufgebaut werden?

Der letztgenannte Punkt soll hier nur insoweit betrachtet werden, als dass darauf hingewiesen werden muss, dass in solchen Fällen MoUs und technische Absprachen zur Synchronisation zwischen den IMS-Betreibern erforderlich sind. Die in Bild 6 von uns vorgeschlagene Lösung konzentriert sich auf die beiden zuerst genannten Probleme der Kommunikation zwischen Endgerät und IMS. Im Mittelpunkt steht dabei ein Webserver (http), welcher vom IMS-Betreiber zur Verfügung gestellt und betrieben wird. Dieser Webserver wird verwendet, um verschiedenste Konfigurations-

Quelle: Inacon GmbH

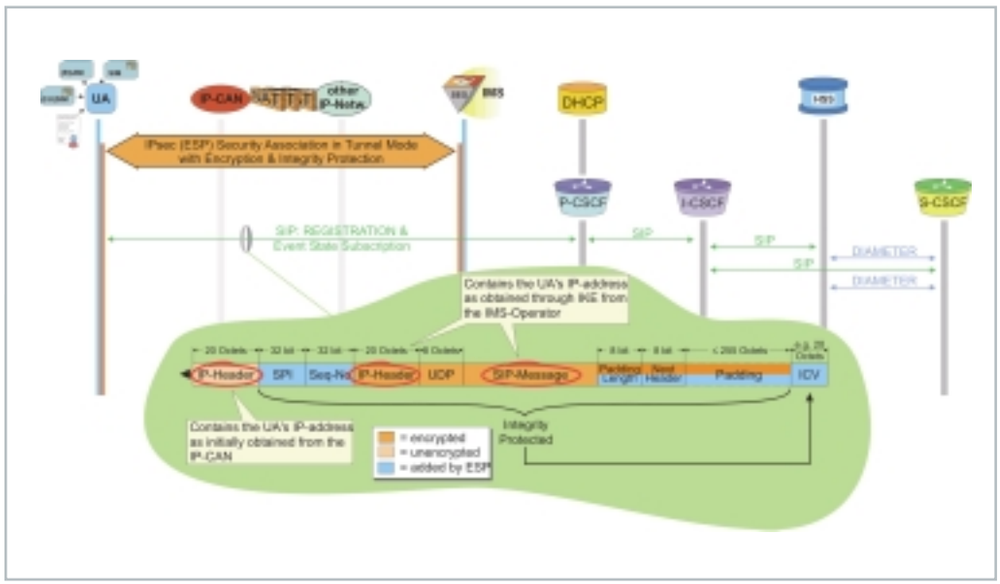


Bild 8: Übersicht der IKEv2-Prozedur aufs IMS angewendet (Teil 1 von 2)

Dateien vom Operator zum Endgerät zu transportieren und zu installieren. Möglich wird diese Lösung durch die Tatsache, dass ein IMS-Roaming zwar technisch möglich ist aber nicht notwendigerweise realisiert werden muss. Vielmehr kann man schon bei der Konfiguration des Endgerätes sicherstellen, dass immer eine so genannte P-CSCF des Heimat-IMS verwendet wird. Die S-CSCF liegt ohnehin immer im Heimat-IMS.

Einen Wermutstropfen gibt es allerdings, und dieser hängt unmittelbar mit dem Problem der Verwendung des Zugangsnetzes eines anderen IMS-Anbieters zusammen: Um QoS vom Zugangsnetz zu bekommen, ist üblicherweise ein so genanntes „Policing“ der angeforderten QoS, beispielsweise zwischen einen Edge-Router beziehungsweise den GGSN auf der einen Seite und die im ersten Teil erwähnte PDF, erforderlich. Soll dies funktionieren, sind die vorher erwähnten MoUs doch erforderlich.

Nun zu den Lösungsansätzen für die Probleme „Verwendung von NAT/NAPT im IP-CAN“; „Intrusion und DoS-Attacken gegen das IMS“; „Identifizierung und Authentisierung des Endkunden beziehungsweise des Endgerätes“ sowie „IPv4- beziehungsweise IPv6-Adressen“. Wiederum eine kurze Wiederholung aus dem ersten Teil zum besseren Verständnis: Das Thema NAT/NAPT ist bei Verwendung von SIP/SDP besonders kritisch, da die eingebetteten privaten IP-Adressen nach dem „NATing“ und außerhalb eines privaten Netzes zum Beispiel für die Registrierung oder fürs Routing von Daten nutzlos sind. Es gibt noch so manch anderes Problem zwischen SIP/SDP und NAT/NAPT, auf die hier aber nicht gesondert eingegangen werden kann. Die im Problem von Intrusion und DoS dargestellten Sicherheitslücken treffen vor allem dann zu, wenn das IMS für beliebige Zugangsnetze geöffnet wird. Was das Thema Identifizierung und Authentifizierung betrifft, so trifft dies immer genau dann zu, wenn SIM-lose Endgeräte verwendet werden sollen. Eigentlich müsste man aber sagen, dass Problem 6 immer dann zuschlägt, wenn beliebige „Credentials“ vom Kunden für die Authentisierung verwendet werden sollen. Schließlich stellt sich auch noch das Problem, ob ein UA (User Agent) IPv4 oder IPv6 oder beides unterstützen muss.

Und hier kommt die Überraschung: All diese Probleme lassen sich durch eine einzige Erweiterung adressieren: Die Verwendung von IKEv2 (Internet Key Exchange Protocol / Version 2 – RFC 4306) im Verein mit EAP-basierten Authentisierungs-Verfahren. Die zugrunde liegende völlig standardkonforme Systemarchitektur ist in Bild 7 generisch dargestellt. Sie zeigt das ehedem offene IMS als „gallisches Dorf“ mit Festungsmauern und IPsec-basierten SEGs (Security Gateway) als Wachtürme. Für unsere Betrachtungen essentiell ist der IPsec-Tunnel zwischen dem links dargestellten SEG und dem User Agent. Mancher wird jetzt einwenden, dass ein IPsec-Tunnel zwischen UA und IMS schon Bestandteil der 3GPP-Release 5 Standards zum IMS gewesen ist. Das ist korrekt, aber mit folgenden Einschränkungen: Laut 3GPP erfordert die Einrichtung eines IPsec-Tunnels zwischen IMS und UA (User Agent) erstens das Vorhandensein einer USIM (Universal Subscriber Identity Module) beim Endkunden beziehungsweise im registrierenden Endgerät, zweitens wird dieser IPsec-Tunnel 3GPP-spezifisch und nicht generisch aufgebaut und, ganz wichtig, er wird aufgebaut zwischen der P-CSCF und dem UA. Was das bedeutet? Ganz einfach: Die von uns im ersten Teil dargestellte DoS-Attacke wird durch das von 3GPP standardisierte Verfahren nicht verhindert. Ganz anders beim hier dargestellten Verfahren: Der IPsec-Tunnel wird zwischen dem UA und einem SEG aufgebaut, bevor der UA überhaupt via SIP mit der P-CSCF korrespondieren darf. Und gegen DoS-Attacken sind SEGs von Hause aus gefeit. Der Aufbau des IPsec-Tunnels zwischen UA und SEG vollzieht sich entsprechend Bild 8 anhand der IKEv2-Prozedur.

Die detaillierte Erläuterung der IKEv2-Prozedur würde an dieser Stelle den Rahmen sprengen aber auf folgende wichtige Details in Bild 8 soll hingewiesen werden:

- Auf Seiten des UA (links oben in Bild 8) erlaubt IKEv2 die Verwendung jeder Art von „Credentials“ für die Authentisierung. Damit ist das Problem der rein SIM-basierten Authentisierung gelöst.
- Der UA beziehungsweise das verwendete IP-Modul (zum Beispiel WLAN- oder die Ethernet-Karte, UMTS-Karte) assoziieren lange vor dem Start von IKEv2 mit dem lokalen IP-basierten Zugangsnetz und erhalten wahrscheinlich eine private IP-Adresse.
- Zum Start der IKEv2-Prozedur ermittelt der UA zunächst via DNS die IP-Adresse des SEG und richtet anschließend via Diffie-Helman eine schon recht sichere IKE-Security Association ein.
- Nachdem man sich so vor unerwünschten Mithörern abgesichert hat, beginnt unterhalb des blauen Doppelpfeils in Bild 8

und bereits verschlüsselt die eigentliche harte Authentisierung mittels EAP-Verfahren. Jeder Typ von „Credential“ kann hier unterstützt werden, es ist reine Konfigurationssache, das Verfahren selbst ändert sich dadurch nicht.

■ Ganz wichtig: Wie viele NAT/NAPT-Router zwischen UA und SEG liegen, spielt für den Erfolg der dargestellten Prozedur keine Rolle. Und, bitte kurz rekapitulieren: Denn bisher wurden überhaupt noch keine SIP-Nachrichten gesendet oder empfangen.

■ Die EAP-basierte Authentisierung endet in jedem Fall mit der Generierung von digitalem Schlüsselmaterial, welches für die Verschlüsselung im eigentlichen IPsec-Tunnel (Tunnel-Modus und ESP) verwendet werden soll, der allerdings ganz unten in Bild 8 überhaupt erst eingerichtet wird.

■ Und besonders reizvoll ist die Tatsache, dass mit Aufsetzen des IPsec-Tunnels der UA die Möglichkeit hat, eine eigene IP-Adresse vom IMS anzufragen. Dies tut man offensichtlich, um das Problem NAT/NAPT zu adressieren, wie im Bild 9 oben gezeigt wird.

■ So ganz nebenbei löst man aber auch das Problem der Ungewissheit, welcher Typ IP-Adresse innerhalb des UA unterstützt werden soll. Ein Operator kann zum Beispiel bestimmen, dass all seine UAs grundsätzlich IPv6 unterstützen sollen und mithilfe von IKEv2 wird dies auch Realität. Die unter dem UA liegende NIC zur puren Herstellung der IP-Konnektivität wird dabei vom eigentlichen UA oder den höheren Schichten entkoppelt.

Nachdem der IPsec-Tunnel (Tunnel-Modus/ESP) aufgesetzt ist, werden sämtliche im Tunnel gesendeten Daten authentisiert, das heißt auf Veränderungen hin überprüft. Dies geschieht mithilfe des ICV am Ende eines solchen Rahmens. Ganz besonders wichtig ist aber auch die Tatsache, dass die orange dargestellten Rahmenteile in Bild 9 zusätzlich verschlüsselt werden. Mit dieser Sicherheit im Hintergrund verliert sich die Notwendigkeit einer SIP-basierten Authentisierung durch das IMS.

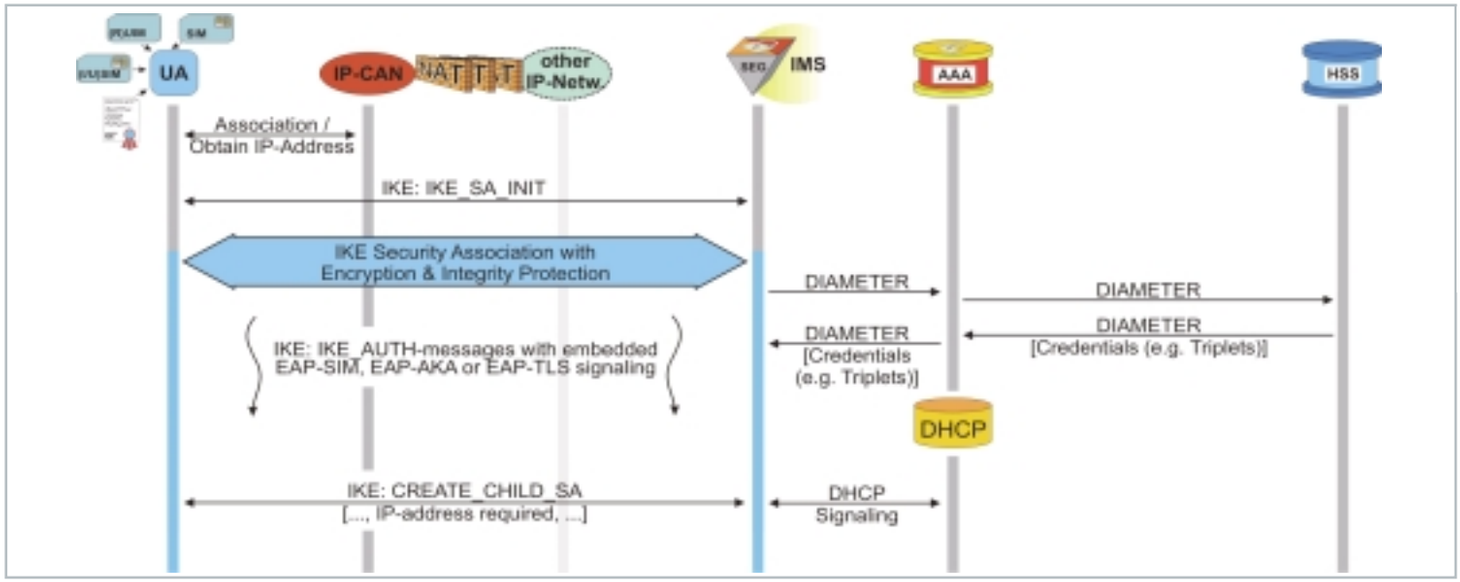
Wie dargestellt lassen sich SIP-Nachrichten in innere UDP/IP-Rahmen verpacken, die den UA mit der vom IMS bezogenen IP-Adresse und auf der Gegenseite die P-CSCF identifizieren. Aufgrund der Verschlüsselung entzieht sich diese Tatsache allerdings jedem möglichen Mithörer zwischen dem UA und dem IMS. Diese inneren IP-Rahmen werden via IPsec komplett verschlüsselt und um eine inkrementale Sequenznummer und einen Pointer (SPI) erweitert. Für diesen Rahmen wird dann der ICV berechnet und ganz hinten an den Rahmen angehängt. Das gesamte Konstrukt wird anschließend in einen äußeren IP-Rahmen gepackt, welcher als IP-Adressen also die private IP-Adresse des UA sowie auch die IP-Adresse des SGW verwenden.

Derselbe Tunnel zwischen UA und P-CSCF wird ebenfalls für Datentransfer eingesetzt, was die Komplexität in den Bereichen Sicherheit und NAT/NAPT-Thematik ganz wesentlich reduziert. Wer sozusagen auf „Nummer Sicher“ gehen möchte, kann den ESP-Rahmen (beginnend mit SPI) noch zusätzlich in UDP einbetten (entsprechend RFC 3948) um in den alten NAT/NAPT-Routern ein Verwerfen der gesamten IP-Rahmen zu verhindern.

Und abschließend sollen noch folgende Vorteile des Verfahrens genannt werden:

■ IKEv2 verfügt über ein eigenes NAT/NAPT-Erkennungssystem, welches zum Beispiel zum Triggern eines wiederum IKEv2-eigenen „Keep-Alive“ zwischen UA und SEG verwendet werden kann. Dadurch wird verhindert, dass die zwischen UA und SEG liegenden NAT/NAPT-Router die Assoziationen zwischen privaten und öffentlichen IP-Addressen und Port-Nummern löschen.

■ IKEv2 ist eine Vorstufe zum so genannten Mobike (Mobility and Multihoming Protocol, RFC 4555). Im Gegensatz zu IKEv2 erlaubt Mobike sogar den unterbrechungsfreien Schwenk des IPsec-Tunnels auf ein anderes IP-CAN, also zum Beispiel von WLAN/DSL auf Wimax oder UMTS. Mit dieser Maßnahme hebt man das Mobilitäts-Management endgültig auf die IP-Ebene.



Quelle: Inacon GmbH

Bild 9: Übersicht der IKEv2-Prozedur aufs IMS angewendet (Teil 2 von 2) sowie Rahmenformat im ESP-Tunnel

Fazit

Ich hoffe, dass Ihnen diese Artikel-Serie beim Lesen ebensoviel Freude bereitet hat wie mir beim Schreiben. Der erste Teil „Das IMS als Herz von NGNs“ erschien in funkschau 4/2007, Seite 28 – 31 und Teil zwei „Probleme bei IMS“ in funkschau 5/2007, Seite 26 – 27. Im Falle von weitergehenden Fragen möchte ich Sie hiermit ermuntern mich per E-Mail (gheine@inacon.de) zu kontaktieren. *(GB)*