Sichere Kommunikation – ein neues Modell und seine Anwendung auf IMS

Andreas Rehbein, Ulrich Trick
Fachhochschule Frankfurt/M. - University of Applied Sciences, Kleiststraße 3, 60318 Frankfurt/M., Germany
E-Mail: rehbein@e-technik.org, trick@e-technik.org;
Steffen Oehler, Murugaraj Shanmugam
Detecon International GmbH, Oberkasseler Straße 2, 53227 Bonn, Germany
E-Mail: Steffen.Oehler@detecon.com, Murugaraj.Shanmugam@detecon.com

Kurzfassung

Durch die Einführung von Multimedia over IP in Mobilfunknetzen der 3. Generation, in NGN-basierten Festnetzen, in konvergenten öffentlichen Netzen sowie dem Internet gibt es neue Sicherheitsrisiken. Daher wurde ein Netzmodell und eine neues Sicherheitsmodell entwickelt, um unterschiedlichste Netz- und Provider-Szenarien beschreiben und analysieren zu können. Darauf basierend können die erforderlichen Sicherheitsmechanismen abgeleitet werden. Die Vorgehensweise hierbei wird beispielhaft an der Zusammenschaltung von UMTS-Netzen mit IMS im Roaming-Fall sowie für Multimedia over Internet aufgezeigt.

1 Einführung

Mit der Einführung von NGN und speziell dem IMS (IP Multimedia Subsystem) wird die Konvergenz von IT- und TK-Welt vorangetrieben. Unabhängig vom Zugangsnetz wie UTRAN (Universal Terrestrial Radio Access Network), WiMAX (Worldwide Interoperability for Microwave Access), WLAN (Wireless Local Area Network) oder anderen werden dem Anwender IP-basiert Provider- und Endgeräte-übergreifend Applikationen zur Verfügung gestellt. Doch diese neuen bzw. erweiterten Möglichkeiten bergen infolge des Internet-Protokolls (IP) erhebliche Sicherheitsrisiken.

Diese Risiken müssen abgeschätzt, die Anforderungen spezifiziert und die notwendigen Sicherheitsmechanismen definiert werden. Dazu werden in einem ersten Schritt die möglichen Provider-Szenarien u.a. unter Berücksichtigung von Roaming modelliert, in einem zweiten Schritt wird dann hierfür basierend auf den Anforderungen ein neues Sicherheitsmodell eingeführt, auf dessen Basis in der Folge die für ein bestimmtes Szenario notwendigen Sicherheitsmechanismen abgeleitet werden können. Da in den zukünftigen Mobilfunk-, Fest- und konvergenten Netzen das IMS eine wichtige Rolle spielt, wird speziell auch darauf eingegangen, welche Sicherheitsmechanismen von den Standardisierungsgremien für das IMS vorgesehen sind, um den neuen Sicherheitsrisiken zu begegnen. Wie sehen notwendige Ergänzungen für Roaming-Szenarien aus? Welche Sicherheitsmechanismen würden benötigt, um einen vergleichbaren Funktionsumfang mit einem ebenso vergleichbaren Sicherheitslevel auf Basis einer Internet-basierten Lösung zu gewährleisten? Diese Fragen werden in diesem Beitrag beleuchtet und geklärt.

2 Anforderungen, Netz- und Sicherheitsmodell

Die Anforderungen an die Sicherheit, die im Zuge der genannten Modellentwicklung festgelegt wurden, sind

- Authentifikation
- Zugriffskontrolle
- Vertraulichkeit
- Integrität
- Verbindlichkeit
- Privatsphäre und
- Verfügbarkeit der Netzinfrastruktur.

Diese Punkte müssen in den verschiedenen Netzen und Netzteilen für Signalisierung und Nutzdaten sowohl aus Nutzer- als auch aus Betreibersicht berücksichtigt werden. Ergänzend hierzu wurden die Randbedingungen „Berücksichtigung von Lawful Interception“ und „Minimierung der Kosten durch möglichst geringe Anzahl an Netzelementen“ einbezogen. Grundsätzlich gilt, dass sich die Überlegungen auf „Multimedia over IP“, nicht auf „IP-Kommunikation allgemein“ beziehen.

Ein neues Netz- (**Bild 1**) und Sicherheitsmodell (**Bild 2**), welches im Rahmen des Forschungs- und Entwicklungsprojekts „Multimedia over IP und Sicherheit“ in Zusammenarbeit mit der Detecon International GmbH entstanden ist, bietet die Möglichkeit der Abbildung von verschiedenen Provider-Szenarien im Hinblick auf die Netzzusammenschaltung verschiedener Anbieter unter der Berücksichtigung von sicherheitsrelevanten Aspekten. Mithilfe der Kombination beider Modelle werden Provider in die Lage versetzt, sich in dem Netzmodell zu positionieren und Informationen bezüglich der Ihnen zur Verfügung stehenden Möglichkeiten zur Sicherung der Nutzerdaten im All-

gemeinen und ferner des eigenen Systems bzw. Netzes einzuholen.

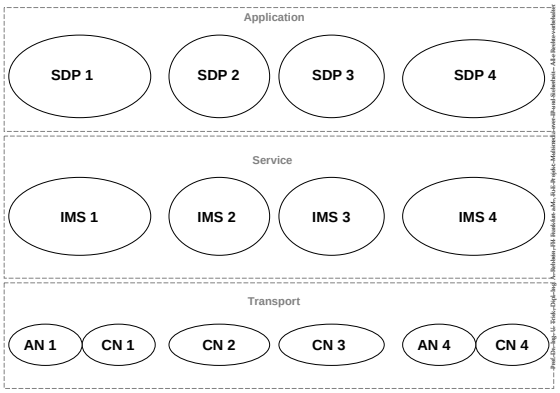

Bild 1 Netzmodell

Das Netzmodell in **Bild 1** bildet die Grundlage zur Betrachtung komplexer Provider-Szenarien. Es teilt die Anbieter im Sinne ihres Angebotes in die drei waagerecht angeordneten Strata Transport, Service und Application ein. So lassen sich Betreiber von Service Delivery Plattformen (SDP, Application Stratum), IMS-Diensteanbieter (IMS, Service Stratum) sowie Zugangs- (AN) und Core-IP-Netzbetreiber (CN) abbilden (Transport Stratum). Verdeutlicht wird dieser Ansatz durch **Bild 3**. Es gilt, dass ein Provider Dienste aus allen drei Strata anbieten kann (Full Service Provider), es ist aber auch möglich, dass die durch die drei Strata modellierten Funktionen von drei oder zwei verschiedenen Providern bereitgestellt werden.

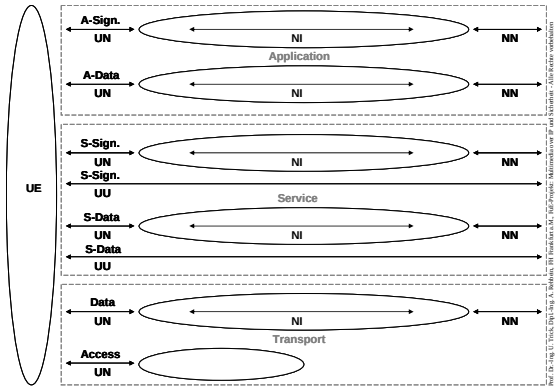

Bild 2 Neues Sicherheitsmodell für Multimedia over IP

Die senkrechte Einteilung in **Bild 1** mit bis zu vier sich aus den genannten drei Strata zusammensetzenden Netzen berücksichtigt auch komplexe Netzszenarien mit einer Vielzahl zusammen geschalteter Netze und Netzteile unter Berücksichtigung von Roaming. Die Betrachtung des umfangreichsten Kommunikationsszenarios für vier zusammen geschaltete NGN/IMS-Netze mit Roaming-Abkommen zwischen den IMS-Providern und dem Aufenthalt zweier Kommunikationspartner/Nutzer in besuchten Netzen begründet die Begrenzung der Anzahl beteiligter Anbieter auf vier.

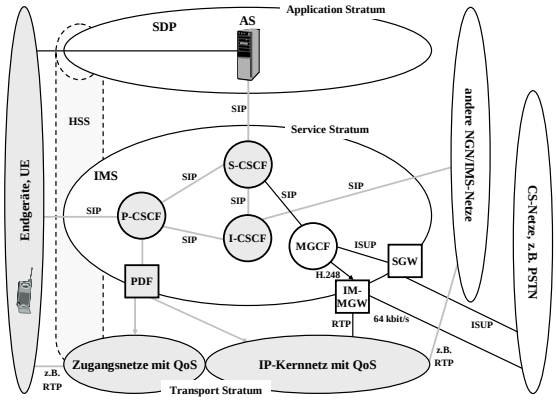

Bild 3 NGN-Architektur in einer Strata-Struktur

Das Sicherheitsmodell in **Bild 2** lehnt sich an die Aufteilung im Netzmodell gemäß der **Bilder 1 und 3** an. Es legt allerdings den Fokus auf die die Sicherheit betreffenden Schnittstellen zwischen Nutzer und Netzwerk (User - Network, UN), denen zu anderen Betreibern (Network - Network, NN) und den internen Netzbereich eines Anbieters (Network Internal, NI). Das Modell gemäß **Bild 2** greift die technische Einteilung aus dem Netzmodell in **Bild 1** auf, um eine Konvergenz beider Modelle zu ermöglichen. Im Hinblick auf die Betrachtung der Sicherheit von Multimedia over IP-Diensten werden unterschiedliche Schnittstellen für Signalisierungs- (Sign.) und Nutzdaten (Data) im Service und Application Stratum definiert.

Netz- und Sicherheitsmodell sind die Basis, um beliebige Netzszenarien unter Berücksichtigung der Anforderungen aus Sicherheitssicht zu modellieren und die erforderlichen Sicherheitsmechanismen abzuleiten. Konkret werden sie hier auf ein IMS-Netzszenario und eine Internet-basierte Lösung angewandt. Daher werden im Folgenden zunächst die Techniken, die zur allgemeinen Gewährleistung der standardisierten IMS-Sicherheitsmechanismen notwendig sind, vorgestellt. Im Zuge dessen werden das angesprochene Netz- und Sicherheitsmodell Anwendung finden, indem die sicherheitsrelevanten Schnittstellen des IMS auf beide Modelle abgebildet werden. Im nächsten Schritt werden die Modelle sowohl auf den komplexesten IMS-Roaming-Fall als auch auf eine vergleichbare Internet-Lösung angewandt und diese abschließend miteinander verglichen.

3 IMS in NGN

Das IMS, dessen Systemarchitektur prinzipiell Bild 3 entnommen werden kann, bietet standardisiert speziell Sicherheitsmechanismen für Authentifizierung, Authorisierung, Integritäts- und Vertraulichkeitsschutz. Diese Mechanismen werden durch verschiedene Techniken und Maßnahmen wie IMS AKA (IMS Authentication and Key Agreement), NDS (Network Domain Security) und SEGs (Security Gateways) bereitgestellt. Welche Funktionen genau und in welchem Maße die einzelnen Mechanismen erfüllen, wird detailliert am IMS-Roaming-Beispiel beschrieben. Darüber hinaus kann selbstverständlich die Verfügbarkeit durch Systemredundanz etc. sichergestellt werden.

IMS Roaming

Der komplexeste IMS-Roaming-Fall (**Bild 4**) sieht die Session-basierte Zusammenschaltung von maximal vier Providern vor. Im Einzelnen sind das der Anbieter des *Visited Networks 1*, in dem sich ein roamender User (UE A) befindet. Dieser ist Kunde des *Home Networks 2*. Er kommuniziert mit einem zweiten User (UE B), welcher Kunde des Anbieters des *Home Networks 3* ist, zum Zeitpunkt des Zustandekommens der Session aber über Anbieter 4, dem Besitzer des *Visited Networks 4*, erreichbar ist.

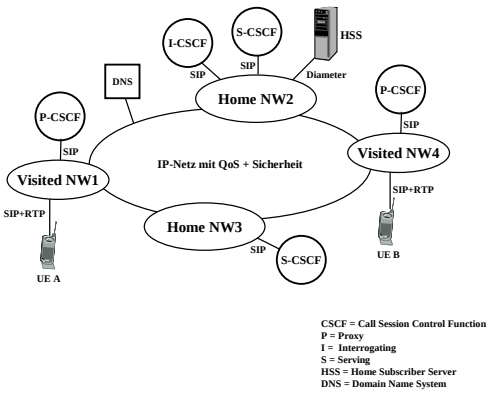

Bild 4 IMS-Roaming-Szenario

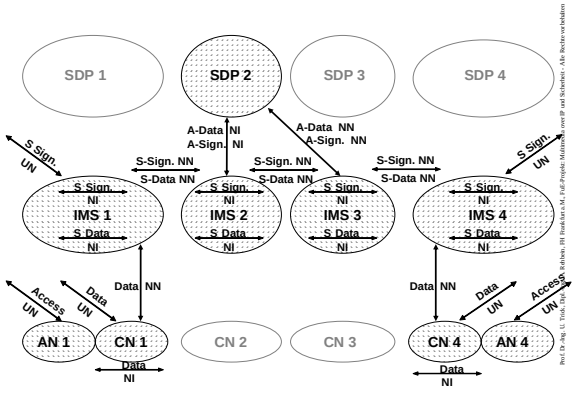

Bild 5 IMS Sicherheitsmechanismen bezogen auf Netzschnittstellen

Durch Abbildung dieses Szenarios auf das Netz- (**Bild 1**) und das Sicherheitsmodell (**Bild 2**) entsteht ein Modell (**Bild 5**), anhand dessen sich die IMS-Sicherheitsmechanismen bezogen auf die Netzschnittstellen darstellen lassen. Diese Mechanismen und deren Einsatzort sind in **Tabelle 1** übersichtlich aufgeführt.

Tabelle 1 IMS-Sicherheitstechniken

Schnittstelle	Technik	
Access UN	IMS AKA	
Data UN	Abhängig vom Zugangsnetz	
Data NI		
Data NN	SEG/NDS	IPsec ESP
S-Data NI	-	
S-Data NN	SEG/NDS	IPsec ESP
S-Sign. UN	IPsec ESP	
S-Sign. NI	IPsec ESP (optional)	
S-Sign. NN	SEG/NDS	IPsec ESP
A-Data NI	-	
A-Data NN	SEG/NDS	IPsec ESP
A-Sign. NI	IPsec ESP (optional)	
A-Sign. NN	SEG/NDS	IPsec ESP

Die Benutzerauthentifikation mittels IMS AKA [1] funktioniert nach den gleichen Richtlinien wie die Authentifizierung im UMTS und bietet demnach auch gegenseitige Authentifizierung Nutzer-Netz und Netz-Nutzer. Nutz- und Signalisierungsdaten werden in den mobilen Zugangsnetzen normalerweise vertraulich behandelt, was jedoch nicht verbindlich ist. IMS hingegen sieht erforderlichen Integritätsschutz und optionale Datenverbindlichkeit vor. Im Zuge der Registrierung werden zwei Paar unidirektionale SAs (Security Associations) erstellt, mit denen diese Anforderungen erfüllt werden und im weiteren Verlauf die SIP-Signalisierung zwischen dem UE und dem P-CSCF mit IPsec ESP [2] geschützt wird. Der Integritätsalgorithmus ist entweder HMAC-MD5 (Hash Message Authentication Code Message-Digest algorithm 5) [3] mit einem 128-Bit-Schlüssel oder HMAC-SHA1 (Secure Hash Algorithm) mit einem 160-bit-Schlüssel. Als Verschlüsselungsalgorithmus können sowohl DES (Data Encryption Standard) E-DE3 (Encrypt-Decrypt-Encrypt3) CBC (Cipher Block Chaining Mode) [4] oder AES (Advanced Encryption Standard) CBC [5] mit 128-Bit-Schlüssel zum Einsatz kommen.

Der Schutz der Mediendaten obliegt dem jeweiligen Zugangsnetz, so werden diese im UTRAN zwischen Mobilgerät und RNC (Radio Network Controller) und im GERAN (GSM EDGE (Enhanced Data Rates for GSM Evolution) Radio Access Network) zwischen Mobilgerät und SGSN (Serving GPRS (General Packet Radio Service) Support Node) verschlüsselt.

SEGs (Security Gateways) befinden sich an den Grenzen zwischen verschiedenen Netzen. Die Schnittstelle zwischen SEGs verschiedener Netze wird als Za und die zwischen dem SEG und eigenen Netzelementen als Zb bezeichnet. Za gewährleistet in jedem Fall Integritäts- und optional Vertraulichkeitsschutz durch einen IPsec ESP Tunnel. Zb schützt die internen Verbindungen mit IPsec ESP (Encapsulating Payload) und bietet ebenfalls mindestens Integrität und optional Vertraulichkeit. Für beide Schnittstellen wird das IKE- (Internet Key Exchange) Protokoll zur Aushandlung, Etablierung und Aufrechterhaltung von ESP SAs (Security Associations) verwendet.

Die IMS Sicherheitstechniken erfüllen die, in Kapitel 2 aufgeführten, Anforderungen an die Sicherheit wie folgt: Die verwandten Anforderungen Authentifikation und Zugriffskontrolle werden durch IMS AKA und Mechanismen des jeweiligen Zugangsnetzes erfüllt. Die ebenso eng miteinander verknüpften Anforderungen Vertraulichkeit, Integrität und Verbindlichkeit (wobei diese auch abhängig von der Authentifikation ist) werden durch SEG/NDS und IPsec gewährleistet. Privatsphäre liefert die Verwendung des SIP-Header-Feld „Privacy“ beschrieben in RFC 3323 [7]. Die Verfügbarkeit wird zum Teil durch SEGs sichergestellt, worauf im Fazit allerdings noch genauer eingegangen wird.

4 Internet

Die gleiche Funktionalität in einer Internet-basierten Lösung inklusive der Roaming-Möglichkeiten angewandt auf Netz- (**Bild 1**) und Sicherheitsmodell (**Bild 2**) führt zur Darstellung in **Bild 6**. Im Gegensatz zum sehr komplexen IMS-Fall sind bei der Internet-Lösung deutlich weniger Netzelemente beteiligt. Zudem funktioniert hier die durch SIP gegebene Mobilitätsunterstützung ohne Roaming-Abkommen zwischen den beteiligten Service-Anbietern. Es existiert nur ein Core-Netzwerk, das öffentliche Internet, zudem sind maximal zwei Service Provider beteiligt.

Auch dieser Fall wird in einer Tabelle (**Tabelle 2**) mit Techniken und Mechanismen, kategorisiert im Bezug auf deren Einsatzort, beschrieben. Da bereits im IMS-Fall aufgrund der zahlreichen Zugangsmöglichkeiten keine eindeutige Festlegung möglich war, und dies im Internet-Fall noch vielfältiger ist, wird der Zugangsbereich nicht zum Vergleich hinzugezogen.

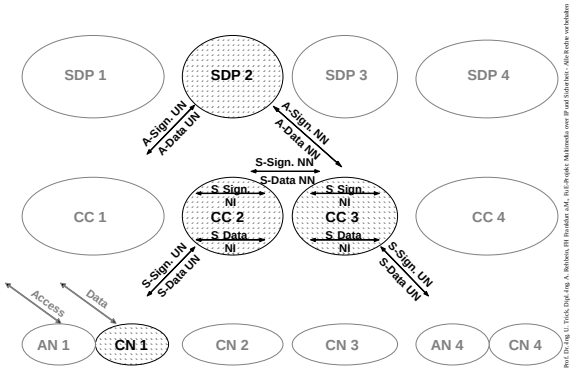

Bild 6 Internet-basierte Lösung bei Multimedia over IP

Mit den in Tabelle 2 angegebenen Techniken könnte sich ein vergleichbarer Sicherheitslevel, gemessen an dem Gesamtkonzept des IMS-Roaming-Falls, erreichen lassen. Für die Verschlüsselung der Nutz- und Signalisierungsdaten könnte TLS (Transport Layer Security) bzw. MTLS (Mutual Transport Layer Security) zum Einsatz kommen. Die Authentifizierung der Nutzer wird mit dem SIP Digest Verfahren [6] und der Schutz der Privatsphäre durch SIP Privacy Services [7] gewährleistet. Die Abgrenzung der verschiedenen Netze untereinander sollte mit SBCs (Session Border Controllern) durchgeführt werden. Sie bieten einen sicheren Übergang zu anderen Netzen und bieten ferner einen möglichen Abgriffspunkt für Lawful Interception und Abrechnung.

Tabelle 2 Techniken zur Sicherung der Internet-Lösung für Multimedia over IP

Schnittstelle	**Technik**		
Access	Abhängig vom Zugangsnetz		
Data			
S-Data UN	TLS für Nutzdaten (TCP) , SRTP (UDP)		
S-Data NN	SBC		
S-Data NI	IPsec		
S-Sign. UN	SIP Digest	Privacy Service RFC 3323	SIPS (MTLS)
S-Sign. NN	SBC		
S-Sign. NI	IPsec		
A-Data UN	TLS für Nutzdaten (TCP) , SRTP (UDP)		
A-Data NN	SBC		
A-Sign. UN	SIP Digest	Privacy Service RFC 3323	SIPS (MTLS)
A-Sign. NN	SBC		

Die Anforderungen an die Sicherheit aus Kapitel 2 Authentifikation und Zugriffskontrolle werden in diesem Fall durch die Verwendung von SIP Digest sichergestellt, hängen allerdings auch von dem jeweiligen Zugangsnetz ab. Vertraulichkeit, Integrität und Verbindlichkeit werden durch die Mechanismen SIPS (Signalisierung), TLS für Nutzdaten (TCP), SRTP (UDP) und der Verwendung von SBCs an den Netzgrenzen (welche ebenfalls in der Lage sind Nutz- und Signalisierungsdaten zu verschlüsseln) erfüllt. Privatsphäre wird ebenso wie im Fall von IMS durch die Verwendung eines SIP Privacy Header-Feld ermöglicht, allerdings können in diesem Fall die SBCs ebenfalls zur Wahrung der Privatsphäre beitragen. Da SBCs ferner eine DoS-Prävention unterstützen, können sie auch die Verfügbarkeit des Systems sichern, wobei dieser Aspekt im Fazit noch einmal aufgegriffen wird.

5 Fazit

Die vorgestellten Modelle für Netzszenarien und die Sicherheit in zusammen geschalteten Netzen ermöglichen strukturierte Sicherheitsbetrachtungen trotz hoher Komplexität. Sie wurden auf zwei konkrete Netzszenarien – mit NGN und IMS bzw. auf Basis Internet – angewandt. Die hierfür erarbeiteten Sicherheitslösungen erfüllen die eingangs erwähnten Anforderungen Authentifikation, Zugriffskontrolle, Vertraulichkeit, Integrität, Verbindlichkeit und die Wahrung der Privatsphäre und bieten eine gute Grundsicherheit. Die standardisierten Mechanismen des IMS sind gut aufeinander abgestimmt, wobei die Sicherheit allerdings auch vom jeweiligen Zugangsnetz abhängt. Das IMS-Konzept ist zudem nicht lückenlos, so werden die Nutzdaten im IMS selbst nicht geschützt, da ein Zugangsnetz wie beispielsweise UTRAN bereits Verschlüsselung der Nutzdaten bietet.

Im Internet-Fall könnte höchstwahrscheinlich eine ebenso hohe Sicherheit gewährleistet werden, wobei natürliche weitergehende Lösungen als die hier vorgestellten möglich sind. Die aufgeführten Empfehlungen für den Internet-Fall sehen im Gegensatz zur IMS-Lösung auch die Verschlüsselung der Nutzdaten im Service-Stratum vor.

Beide Lösungen genügen nicht vollständig der letztgenannten Anforderung, einer hohen Verfügbarkeit der Netzinfrastruktur. Diese lässt sich nur mit zusätzlichen Komponenten wie Intrusion Detection (IDS) oder Intrusion Prevention System (IPS) und, aus der reinen IP-Welt bekannten, Konzepten zur Angriffsabwehr und mit redundanten Systemen gewährleisten.

Die wichtigste Voraussetzung für die Interaktion zwischen verschiedenen Anbietern ist deren Kooperationsbereitschaft. Diese Problemstellung betrifft allerdings beide vorgestellten Fälle, wobei der Aufwand im Falle des Internets – nicht zuletzt aufgrund möglicher Vermittlungsnetzbetreiber – vermutlich geringer ist. Es müssen keine Roaming-Abkommen geschlossen werden.

6 Literatur

[1] TS 33.203: 3G security: Access security for IP-based services; Release 7. 3GPP, März 2007

[2] Kent, S.; Atkinson R.: RFC 2406 - IP Encapsulating Security Payload (ESP). IETF, November 1998

[3] Rivest, R.: RFC 1321 - The MD5 Message-Digest Algorithm. IETF, April 1992

[4] Pereira, R.; Adams, R.: RFC 2451 - The ESP CBC-Mode Cipher Algorithms. IETF, November 1998

[5] Frankel, S.; Glen, R.; Kelly, S.: RFC 3602 - The AES-CBC Cipher Algorithm and Its Use with IPsec. IETF, September 2003

[6] Franks, J.; Hallam-Baker, P.; Hostetler, J.; Lawrence, S.; Leach, P.; Luotonen, A.; Stewart, L.: RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication. IETF, June 1999

[7] Peterson, J.: RFC 3323 - A Privacy Mechanism for the Session Initiation Protocol (SIP). IETF, November 2002